

# Reducing the CNOT count for Clifford+T circuits on NISQ architectures

Vlad Gheorghiu <sup>\*1,4</sup>, Jiaxin Huang <sup>†5</sup>, Sarah Meng Li <sup>‡1,2</sup>, Michele Mosca <sup>§1,2,3,4</sup>, and Priyanka Mukhopadhyay <sup>¶1,2</sup>

<sup>1</sup>Institute for Quantum Computing, University of Waterloo, Waterloo ON, Canada

<sup>2</sup>Department of Combinatorics and Optimization, University of Waterloo, Waterloo ON, Canada

<sup>3</sup>Perimeter Institute for Theoretical Physics, Waterloo, Waterloo ON, Canada

<sup>4</sup>softwareQ Inc., Kitchener ON, Canada

<sup>5</sup>Faculty of Mathematics, University of Waterloo, Canada

May 2, 2022

## Abstract

While mapping a quantum circuit to the physical layer one has to consider the numerous constraints imposed by the underlying hardware architecture. Connectivity of the physical qubits is one such constraint that restricts two-qubit operations, such as CNOT, to “connected” qubits. SWAP gates can be used to place the logical qubits on admissible physical qubits, but they entail a significant increase in CNOT-count. In this paper we consider the problem of reducing the CNOT-count in Clifford+T circuits on connectivity constrained architectures, like noisy intermediate-scale quantum (NISQ) computing devices. We “slice” the circuit at the position of Hadamard gates and “build” the intermediate {CNOT, T} sub-circuits using Steiner trees, significantly improving on previous methods. We compared the performance of our algorithms while mapping different benchmark and random circuits to some well-known architectures such as 9-qubit square grid, 16-qubit square grid, Rigetti 16-qubit Aspen, 16-qubit IBM QX5 and 20-qubit IBM Tokyo. Our methods give less CNOT-count compared to Qiskit transpiler as well as using SWAP gates. Assuming most of the errors in a NISQ circuit implementation are due to CNOT errors, then our method would allow circuits with few times more CNOT gates be reliably implemented than the previous methods would permit.

## 1 Introduction

Quantum computing is a computational paradigm which is predicted to provide significant speedups for problems including, but not limited to, large number factorization [47], simulation of quantum

---

<sup>\*</sup>vlad.gheorghiu@uwaterloo.ca

<sup>†</sup>j2huang@uwaterloo.ca

<sup>‡</sup>sarah.li@dal.ca

<sup>§</sup>michele.mosca@uwaterloo.ca

<sup>¶</sup>mukhopadhyay.priyanka@gmail.com, p3mukhop@uwaterloo.ca

systems [14] and unstructured search [17], all of which are believed to be intractable or significantly slower on a classical computer. Somewhat similar to its classical counterpart, a quantum circuit consisting of elementary unitary operations remains the most popular model for quantum computation. Thus we need efficient quantum compilers that map a high-level algorithm into a lower-level form, that is, a quantum circuit consisting of quantum gates that are admissible by the hardware constraints.

At present we do not have large-scale quantum computers. Rather the devices available today are referred to as noisy intermediate-scale quantum (NISQ) computers [38]. The current technologies that realize these devices, such as superconducting quantum circuits [43, 56] and ion traps [8, 6, 18, 20], impose certain connectivity constraints by which two-qubit operations are possible only among certain pairs of physical qubits. Naively we can insert SWAP operators to move a pair of logical<sup>1</sup> qubits to physical positions admissible for two-qubit operations. However, this increases the number of two-qubit operations, each of which again introduces non-negligible noise. Hence, it is important to optimize the number of two-qubit operators while respecting the connectivity constraints.

In this paper we consider the problem of re-synthesizing a circuit over the universal fault-tolerant Clifford+T gate set. We designed and implemented an algorithm that reduces the number of CNOT gates required to meet the connectivity constraints imposed by the physical hardware architectures. The connectivity constraints are represented in the form of a graph  $G$  (called **connectivity graph**) in which the vertices represent (physical) qubits and a two-qubit operation can be applied if and only if the corresponding vertices are connected by an edge in  $G$ . We assume without loss of generality that the desired circuit is connected (that is, we can't break it up into non-interacting collections of qubits).

The Clifford+T gate set is one of the most studied fault-tolerant universal gate set used to realize a quantum operator. We consider the following gates in this set:  $\mathcal{G}_{univ} = \{\text{CNOT}, \text{H}, \text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{X}, \text{Y}, \text{Z}\}$ , among which CNOT is the only multi-qubit operator. If the shortest path length between vertices corresponding to  $c$  and  $t$  in  $G$  is  $\ell$ , then the naive way of using SWAP gates (equivalent to 3 CNOT gates) would require about  $6(\ell - 1)$  CNOT gates (Figure 1).

Thus we devise algorithms using Steiner trees that reduce the number of CNOT gates. Steiner trees were also used in [34] and [26] for the similar goal of reducing CNOT gates. Our algorithms differ from these works, which we have pointed out in the following paragraphs, and give much less CNOT-count.

## Our techniques

Our approach can be described as *slice-and-build*. Given a circuit  $\mathcal{C}_I$  as a sequence of gates we slice it at “suitable” points and re-synthesize or build the intermediate sliced portions in a manner such that connectivity constraints are respected and at the same time we tried to reduce the number of CNOT gates. We have described two methods for *slice-and-build*.

The first procedure, CNOT-OPT-A (Algorithm 5) described in Section 4.1, has a simple slicing technique. We partition the circuit  $\mathcal{C}_I$  at the position of the Hadamard (H) gates. Each intermediate sub-circuit composed of the gates  $\mathcal{G}_{ph} = \mathcal{G}_{univ} \setminus \{\text{H}\}$  is re-synthesized using algorithms PHASE-NW-SYNTH (Algorithm 4) and LINEAR-TF-SYNTH (Algorithm 1). For each sub-circuit we

---

<sup>1</sup>In NISQ systems, a “logical qubit” typically corresponds to a single individual qubit, in contrast to fault-tolerant quantum computation where a logical qubit is encoded in many physical qubits. However, the correspondence between the logical qubits and physical qubits on a NISQ computer can change throughout the computation.

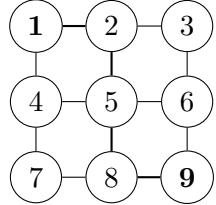


Figure (a): 9-qubit square grid

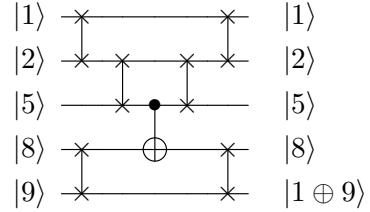


Figure (b):  $CNOT_{1,9}$  with SWAPs

Figure 1: In the SWAP template SWAP gates are placed along the shortest path between two qubits on the given connectivity graph, in this case a 9-qubit square grid (Fig a). When the required logical qubits are on adjacent physical qubits (Fig b) then CNOT is applied. SWAP gates are again placed to get the correct logical value on all physical qubits.

first calculate the phase polynomial  $\mathcal{P}$  and overall linear transformation  $\mathbf{A}_{slice}$ . We synthesize a phase polynomial network circuit  $\mathcal{C}_{ph}$  with the gates in  $\mathcal{G}_{ph}$ , using PHASE-NW-SYNTH (Algorithm 4) described in Section 3.2. The algorithm draws inspiration from the parity network synthesis algorithm in [1]. We calculate the *parity network matrix* in which each column stores a parity term. The aim is to apply a series of transformations (CNOT gates) such that each parity term occurs at least once in the circuit. Then depending on the coefficients of the parity terms we place the gates in  $\mathcal{G}_{ph} \setminus \{CNOT, X\}$ . To impose connectivity constraints we construct Steiner trees (Section 2.3) with terminals being the set of qubits (or vertices) satisfying certain conditions. Then depending on the edge information, we perform a series of CNOT operations to get the desired result. We emphasize that our way of placing CNOT gates according to the Steiner tree edges is different from that described in [34]. In [26] the authors remarked that Steiner trees can be used for synthesizing a circuit from its phase polynomial, but no detail was given.

The phase polynomial network corresponding to  $\mathcal{P}$  has some overall transformation  $\mathbf{A}_{ph}$ . We synthesize a circuit  $\mathcal{C}_{lin}$  that implements the “residual” linear transformation  $\mathbf{A} = \mathbf{A}_{ph}^{-1} \mathbf{A}_{slice}$  using LINEAR-TF-SYNTH (Algorithm 1), described in Section 3.1. The main motivation of this algorithm comes from the work in [37] that synthesizes a linear reversible circuit using CNOT gates. We follow the same reverse-engineering procedure where we (i) reduce  $\mathbf{A}$  first to an upper triangular form, (ii) transpose the result and then (iii) reduce it to a lower triangular form so that we get the identity matrix  $\mathbb{I}$ . Each linear operation corresponds to a CNOT gate and connectivity constraints are imposed by constructing series of Steiner trees. Our procedures at steps (i) and (iii) differ from the approach in [34, 26], and we also get less CNOT-count.

In our second procedure CNOT-OPT-B (Algorithm 6) described in Section 4.2, the slicing points remain the H gates but the set that is partitioned is the phase polynomial  $\mathcal{P}_I$  of the entire circuit  $\mathcal{C}_I$ . Between two H gates (including the ends) we synthesize a phase polynomial network circuit using gates in  $\mathcal{G}_{ph}$  that realizes the partial phase polynomial  $\mathcal{P}_{sub}$ , comprising of terms in  $\mathcal{P}$  that become uncomputable after the H gate being placed at the end of the current slice. Here it must be noted that by the *sum-over-paths* formulation (Section 2.2) new *path variables* are introduced after application of each H gate. This renders some terms of the phase polynomial uncomputable after certain points in the circuit. The synthesis of phase polynomial network is done using PHASE-NW-SYNTH (Algorithm 4). Let  $\mathbf{A}_{slice}$  be the transformation that maps the state of the qubits in  $\mathcal{C}_I$  after the H gate at the beginning of a slice to the state of the qubits in  $\mathcal{C}_I$  before the H

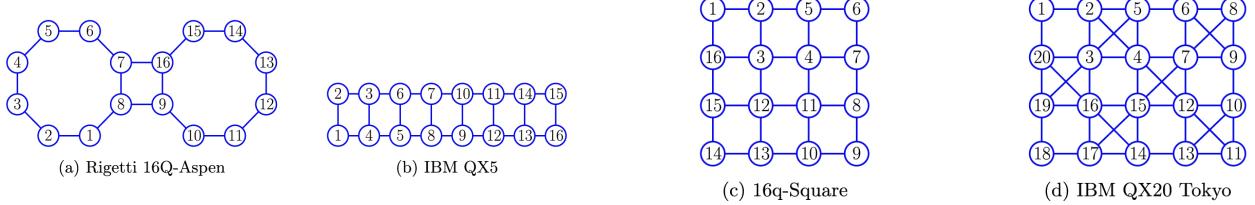


Figure 2: Connectivity graphs of some architectures that have been implemented in practice. Images taken from [11].

gate at the end of the slice. We synthesize a circuit implementing  $\mathbf{A} = \mathbf{A}_{ph}^{-1} \mathbf{A}_{slice}$  using LINEAR-TF-SYNTH (Algorithm 1) such that between any two H gates (as well as at the ends) the linear transformation  $\mathbf{A}_{slice}$  remain unchanged. A similar kind of partitioning of the circuit according to the phase polynomial was used in [3] where the goal was to reduce T-depth of the input circuit.

## Our results

We have re-synthesized some benchmark as well as randomly generated circuits after taking into account connectivity constraints imposed by the architectures (which have been implemented in practice) shown in Figure 1 and 2. Here we emphasize that we have studied the performance of our procedures as baseline algorithms. The results will likely improve if coupled with some other procedures that handle the problem of optimal initial mapping of qubits. To be precise, we have considered only one mapping where qubit  $i$  is mapped to vertex  $i$  of the given connectivity graphs. Considerable amount of work has been done, which considers the optimal mapping that reduces the resources required. So if such a procedure is done as pre-processing, then the CNOT-count will likely reduce further. We have compared the CNOT-count overhead, that is, the increase in CNOT-count obtained from our algorithms with the overhead obtained using SWAP-template (Figure 1) and Qiskit transpiler. We have observed that both our algorithms give remarkable improvement in the case of benchmark circuits (Table 2 in Section 4.3). In case of random circuits we have found that the simple way of slicing in CNOT-OPT-A gives much less overhead (Table 1 in Section 4.3). CNOT-OPT-B, however, fares poorly in many cases.

### 1.1 Related work

There have been quite a number of works that deal with the problem of CNOT optimization without taking into account the connectivity constraints imposed by the underlying hardware architecture, for example, [22, 49, 37, 48, 35, 59, 1].

Some authors [29, 39, 61, 23, 24] use SWAP gates along with some gate commutation and transformation rules to obtain a circuit that respect connectivity constraints. There are algorithms that take advantage of the restricted topology such as 1D linear nearest neighbor ([33, 19, 53, 10, 51, 42]), hypercubic [7] which rely on classical sorting networks and 2D grid ([52, 30, 61, 41]). Some algorithms that work on general topology for NISQ devices are [62, 4, 50, 29, 9, 58]. Broadly, these algorithms use qubit mapping technique to search for the optimal placement of SWAP gates and qubits. The search space scales exponentially for exact algorithms such as [55, 31], making them impractical for large NISQ devices. Thus, some authors [9, 29, 40] use heuristics to reduce the search space. Some of these heuristics algorithms, e.g. [62], which is based on depth partitioning

and  $A^*$  search, are developed for specialized architectures such IBM devices. In [13] the authors give an approach for realizing arbitrary parity-function oracles, while taking care of the underlying topology. It has been shown in [36] that the size of the resulting circuit is very sensitive to the original placement of the logical qubits on the device.

To reduce CNOT-count, Steiner trees have been used in [26, 34, 60, 54], while in [11] the problem is reduced to a well-known cryptographic problem - the syndrome decoding problem.

## 1.2 Organization

After giving some preliminaries in Section 2 we describe our algorithms in Section 3 and 4. The algorithms LINEAR-TF-SYNTH and PHASE-NW-SYNTH that synthesize linear reversible circuits and phase polynomial network circuits are given in Section 3.1 and 3.2 respectively. The algorithms CNOT-OPT-A and CNOT-OPT-B that synthesize the complete circuit over the Clifford+T gate set is described in Section 4.1 and 4.2 respectively. Finally we conclude in Section 5.

## 2 Preliminaries

We write  $N = 2^n$  and  $[K] = \{1, 2, \dots, K\}$ . The  $(i, j)^{th}$  entry of any matrix  $M$  is denoted by  $M_{i,j}$  or  $M_{ij}$  or  $M[i, j]$ . We denote the  $i^{th}$  row of  $M$  by  $M[i, .]$  and the  $j^{th}$  column by  $M[., j]$ . We denote the  $n \times n$  identity matrix by  $\mathbb{I}_n$  or  $\mathbb{I}$  if the dimension is clear from the context. The set of  $n$ -qubit unitaries of size  $2^n \times 2^n$  is denoted by  $\mathcal{U}(2^n)$  or  $\mathcal{U}_n$ .

### 2.1 Cliffords and Paulis

The *single qubit Pauli matrices* are as follows:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (1)$$

The *n-qubit Pauli operators* are :

$$\mathcal{P}_n = \{Q_1 \otimes Q_2 \otimes \dots \otimes Q_n : Q_i \in \{\mathbb{I}, X, Y, Z\}\}. \quad (2)$$

The *single-qubit Clifford group*  $\mathcal{C}_1$  is generated by the Hadamard and phase gate

$$\mathcal{C}_1 = \langle H, S \rangle \quad (3)$$

where

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad (4)$$

When  $n > 1$  the *n-qubit Clifford group*  $\mathcal{C}_n$  is generated by these two gates (acting on any of the  $n$  qubits) along with the two-qubit  $\text{CNOT} = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes X$  gate (acting on any pair of qubits). We write  $\text{CNOT}_{c,t}$  to denote the CNOT gate applied between qubit  $c$  (*control*) and  $t$  (*target*). The logic realized by this gate is :  $\text{CNOT}|c, t\rangle = |c, c \oplus t\rangle$ .

The *Clifford+T* gate set consists of the  $n$ -qubit Clifford group gates along with the T gate, where

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}. \quad (5)$$

It is easy to verify that this set is a group since the H and CNOT gates are their own inverses and  $T^{-1} = T^7$ . Here we note  $S = T^2$ . For  $n > 1$  qubits a minimal generating set for this group is  $\{H, T, \text{CNOT}\}$ .

## 2.2 Circuit-polynomial correspondence

The circuit-polynomial correspondence [32] associates a *phase polynomial* and a linear Boolean transformation with every quantum circuit generated by the set  $\{\text{CNOT}, H, T\}$ . More precisely,

**Lemma 2.1** ([3]). *A unitary  $U \in \mathcal{U}(2^n)$  is exactly implementable by an  $n$ -qubit circuit over  $\{\text{CNOT}, T\}$  if and only if*

$$U |x_1 x_2 \dots x_n\rangle = \omega^{p(x_1, x_2, \dots, x_n)} |g(x_1, x_2, \dots, x_n)\rangle$$

where  $\omega = e^{i\frac{\pi}{4}}$ ,  $x_1, x_2, \dots, x_n \in \mathbb{F}_2$  and

$$p(x_1, x_2, \dots, x_n) = \sum_{i=1}^{\ell} c_i \cdot f_i(x_1, x_2, \dots, x_n)$$

for some linear reversible function  $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  and linear Boolean functions  $f_1, f_2, \dots, f_\ell \in (\mathbb{F}_2^n)^*$  with coefficients  $c_1, c_2, \dots, c_\ell \in \mathbb{Z}_8$ .

For convenience, the set of  $n$ -ary linear Boolean functions  $\mathbb{F}_2^n \rightarrow \mathbb{F}_2$  is referred to as the *dual vector space*  $(\mathbb{F}_2^n)^*$  of  $\mathbb{F}_2^n$ .

This is called the *sum-over-paths* form of a circuit [12, 27, 32] and the variables  $x_1, x_2, \dots, x_n$  are called the *path variables*.  $p(x_1, x_2, \dots, x_n)$  is referred to as the *phase polynomial*. Each  $f_i(x_1, \dots, x_n)$  is a *parity term*.

Thus we can fully characterize a unitary  $U \in \mathcal{U}(2^n)$  implemented by a  $\{\text{CNOT}, T\}$ -generated circuit with a set  $\mathcal{P} \subseteq \mathbb{Z}_8 \times (\mathbb{F}_2^n)^*$  of linear Boolean functions together with coefficients in  $\mathbb{Z}_8$  and a linear reversible output functions  $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ , with the interpretation

$$U_{\langle \mathcal{P}, g \rangle} : |x_1 x_2 \dots x_n\rangle \rightarrow \omega^{\sum_{(c, f) \in \mathcal{P}} c \cdot f(x_1, x_2, \dots, x_n)} |g(x_1, x_2, \dots, x_n)\rangle. \quad (6)$$

The set  $\mathcal{P}$  (*phase polynomial set*) and  $g$  are efficiently computable given a circuit over  $\{\text{CNOT}, T\}$ , taking time linear in the number of qubits and gates.

The H gate is a “branching gate” and has the following effect on a basis state  $x_1 \in \mathbb{F}_2$ .

$$H : |x_1\rangle \rightarrow \frac{1}{\sqrt{2}} \sum_{x_2 \in \mathbb{F}_2} \omega^{4 \cdot x_1 \cdot x_2} |x_2\rangle$$

Here  $x_2$  is the new path variable and the variable  $x_1$  ceases to exist after H is applied. Similar to Lemma 2.1 we can have the following result.

**Lemma 2.2** ([3]). *If a unitary  $U \in \mathcal{U}(2^n)$  is exactly implementable by an  $n$ -qubit circuit over  $\{CNOT, H, T\}$  with  $k$   $H$  gates, then for  $x_1 x_2 \dots x_n \in \mathbb{F}_2^n$ ,*

$$U |x_1 x_2 \dots x_n\rangle = \frac{1}{\sqrt{2^k}} \sum_{x_{n+1} \dots x_{n+k} \in \mathbb{F}_2^k} \omega^{p(x_1, x_2, \dots, x_{n+k})} |y_1 y_2 \dots y_n\rangle$$

where  $y_i = h_i(x_1, x_2, \dots, x_{n+k})$  and

$$p(x_1, x_2, \dots, x_{n+k}) = \sum_{i=1}^{\ell} c_i \cdot f_i(x_1, \dots, x_{n+k}) + 4 \cdot \sum_{i=1}^k x_{n+i} \cdot g_i(x_1, \dots, x_{n+k})$$

for some linear Boolean functions  $h_i, f_i, g_i$  and coefficients  $c_i \in \mathbb{Z}_8$ . The  $k$  path variables  $x_{n+1}, \dots, x_{n+k}$  result from the application of Hadamard gates.

But, unlike Lemma 2.1, the converse is not true.

### 2.3 Steiner tree

A **graph** is a pair  $G = (V_G, E_G)$  where  $V_G$  is a set of *vertices* and  $E_G$  is a set of pairs  $e = (u, v)$  such that  $u, v \in V_G$ . Each such pair is called an *edge*. One may define a function  $w_{E_G} : E_G \rightarrow \mathbb{R}$  that assigns a *weight* to each edge. The graphs we consider are *simple* (with at most one edge between two distinct vertices and no self-loops i.e.  $(u, u) \notin E_G$ ), *undirected* (edges have no direction i.e.  $(u, v) \equiv (v, u)$ ) with edge-weight 1, that is,  $w_{E_G}(e) = 1$  for every  $e \in E_G$ . A graph  $G' = (V'_G, E'_G)$  is a *subgraph* of  $G$  such that  $V'_G \subseteq V_G$  and  $E'_G \subseteq E_G$ . A **tree** is an undirected graph in which any two vertices are connected by exactly one path, or equivalently a connected, acyclic, undirected graph.

**Definition 2.1 (Steiner tree).** Given a graph  $G = (V_G, E_G)$  with a weight function  $w_E$  and a set of vertices  $\mathcal{S} \subseteq V_G$ , a Steiner tree  $T = (V_T, E_T)$  is a minimum weight tree that is a subgraph of  $G$  such that  $\mathcal{S} \subseteq V_T$ .

The set of vertices in  $\mathcal{S}$  are called *terminals* while those in  $V_T \setminus \mathcal{S}$  are called *Steiner nodes*.

Computing Steiner trees is NP-hard and the related decision problem is NP-complete [25]. There are a number of heuristic algorithms that compute approximate Steiner trees [45, 5], the latter giving a solution which is within a factor of 1.39 times the optimal. A survey about different Steiner tree approximation algorithms is given in [21]. The choice of algorithm is usually determined by the application, and typically involves a trade-off between quality (approximation factor) and running time.

The heuristic algorithm we use is the one given by Wang [57], which has similarity to Kruskal's minimum spanning tree algorithm [28]. Similar to [46] we incorporate optimization steps by Rayward et al.[44]. This helps us achieve a better running time compared to the best (with respect to quality) approximation algorithms in the literature, without sacrificing the approximation factor much. The primary idea of the algorithm is to maintain a number of subgraphs and sequentially merge those which are closest to each other. The distance between two subgraphs  $g_i, g_j$  is measured by the length of the shortest path between any two nodes  $u, v$  such that  $u \in V_{g_i} \setminus V_{g_j}$  and  $v \in V_{g_j} \setminus V_{g_i}$ . When a subgraph has all terminals then we stop the merging and remove all non-terminal nodes of degree 1. A pseudocode of this algorithm has been given in Appendix A (Algorithm 7).

The size of the constructed Steiner tree is at most  $2(1 - \frac{1}{\ell})$  times the size of the minimal Steiner tree, where  $\ell$  is the number of leaves in the minimal Steiner tree. The running time is  $O(|\mathcal{S}|^2 (|V_G| + |E_G|))$  [46].

### 3 Synthesis algorithms with connectivity constraint

In this section first we describe a synthesis algorithm that generates a circuit implementing a linear transformation using gates in the set  $\mathcal{G}_{lin} = \{\text{CNOT}, \text{X}\}$  (Section 3.1). Then we describe an algorithm that synthesizes a circuit implementing a phase polynomial network using gates  $\mathcal{G}_{ph}$  generated by the set  $\{\text{CNOT}, \text{X}, \text{T}\}$ .

#### 3.1 Synthesis of $\{\text{CNOT}, \text{X}\}$ circuits

Consider an  $n$ -qubit circuit built with gates in the set  $\mathcal{G}_{lin} = \{\text{CNOT}, \text{X}\}$ . We represent the overall linear transformation by an  $n \times n + 1$  “augmented” matrix  $\mathbf{A} = [\mathbf{A}'_{n \times n} | \mathbf{b}_{n \times 1}]$ , whose rows represent or are indexed by qubits. If we label the initial states of the qubits by variables  $x_1, \dots, x_n$  then the first  $n$  columns represent these variables and the last column represent the variable  $b$  indicating bit flips. Each variable  $x_1, \dots, x_n, b$  takes values from the set  $\{0, 1\}$ . The initial state of  $\mathbf{A}$  is  $[\mathbb{I}_n | \mathbf{0}_{n \times 1}]_{n \times n+1}$ . This represents the initial state of all the qubits. When  $\text{CNOT}_{j,i}$  is applied row  $j$  is added (mod 2) to row  $i$  (row  $j$  remains same). The parity at qubit  $i$  is  $x_i \oplus x_j$ . When an X gate is applied on qubit  $i$  then  $A_{i,n+1} \leftarrow 1 \oplus A_{i,n+1}$ .

Now suppose we are given a linear transformation  $\mathbf{A} = [\mathbf{A}'_{n \times n} | \mathbf{b}_{n \times 1}]$  of a circuit and we want to synthesise a circuit implementing this transformation. We use the same reverse engineering idea of Patel, Markov and Hayes [37]. The procedure is similar to Gaussian elimination. (a) First we make  $\mathbf{b} = \mathbf{0}$  by flipping the entries with 1. This corresponds to applying X on the respective qubit. (b) We apply a series of elementary row operations (bit-wise addition) on  $\mathbf{A}$  such that  $\mathbf{A}'$  is in upper triangular form. Each row operation represents the application of a CNOT gate. (c) Then we transpose the matrix and perform elementary row operations on  $\mathbf{A}^T$  such that  $\mathbf{A}'$  is  $\mathbb{I}$ . The output circuit is constructed as follows : first, the CNOT gates obtained in (c) with the control-target flipped but preserving the order, then the CNOT gates obtained in (b) with control-target preserved but reversing the order in which they were performed, and lastly the X gates obtained in (a).

To incorporate connectivity constraints we use Steiner trees as described in LINEAR-TF-SYNTH (Algorithm 1). We first make  $\mathbf{b} = \mathbf{0}$  by placing X gates (step 2), as described before. Then we convert  $\mathbf{A}'$  into an upper triangular form (step 8) by row-operations “permitted” by the input connectivity graph  $G$ . This is a graph whose vertices represent qubits and a two-qubit gate such as CNOT can be placed only when there exists an edge between the corresponding vertices. For each column of  $\mathbf{A}'$  (starting from the first one) we compute a minimal Steiner tree approximation with (i) connectivity graph  $G' = G \setminus I$  (excluding the vertices in  $I$  and the edges adjacent to these vertices) where  $I$  is the set of columns which have been operated on or which have been “fixed” to have 1 in the diagonal and 0 in the rest, and (ii) set of terminals  $\mathcal{S}$  which are the rows below the diagonal and having a 1. Then we invoke the procedure ROW-OP, as described in Algorithm 2.

The idea of ROW-OP is to use a set of operations such that 1 in the diagonal is “propagated” via intermediate Steiner nodes to cancel the 1 in the terminal nodes and then use another set of operations to cancel any 1s in the Steiner nodes. We assume the diagonal has 1, else it is adjusted by a set of operations to propagate a 1 to the diagonal node (step 4 of Algorithm 1). The diagonal node (let’s call it  $c$ ) becomes the “pivot” node. The input Steiner tree approximation  $T_{c,\mathcal{S}}$  is separated into a set of sub-trees (step 1 of Algorithm 2) by calling the procedure SEPARATE (Algorithm 3). The root and leaves in each such sub-tree are terminal nodes (from  $\mathcal{S}$ ) and the rest are Steiner nodes. Then the 1 from the root of each sub-tree cancels the 1 at the leaves via

---

**Algorithm 1:** LINEAR-TF-SYNTH

---

**Input:** (i) Linear transformation matrix  $\mathbf{A}_{n \times n+1} = [\mathbf{A}'_{n \times n} | \mathbf{b}_{n \times 1}]$ , (ii) Connectivity graph  $G$ .

**Output:** A circuit over  $\{\text{CNOT}, \text{X}\}$  realizing  $\mathbf{A}$ .

```

1  $\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{X} \leftarrow \emptyset, G' \leftarrow G$                                 // Make a copy of  $G$  ;
2 If  $A_{n+1,i} = 1$  then  $\mathcal{X}.\text{append}(X_i)$  and  $A_{n+1,i} \leftarrow 0$  ;
3 for columns  $i = 1 \dots, n$  do
4   If  $A_{ii} = 0$ , find all rows  $j (j > i)$  such that  $A_{ji} = 1$ . Choose  $j$  with the shortest path (in  $G'$ ) to  $i$ .
    Suppose  $i$  is the root and  $j$  is the leaf.  $\mathcal{Y}_1.\text{append}(\text{CNOT}_{uv})$  if  $u$  is the child of  $v$ .
     $\mathbf{A}[v, :] \leftarrow \mathbf{A}[v, :] \oplus \mathbf{A}[u, :]$  ;
5    $\mathcal{S}' = \{j : j > i \text{ and } A_{j,i} = 1\}, \mathcal{S} \leftarrow \mathcal{S}' \cup \{i\}$ .                                //  $\mathcal{S}$  is the set of terminals. ;
6   Find a minimum Steiner tree approximation with connectivity graph  $G'$  and terminals  $\mathcal{S}$ . Let  $i$  be the
      root of this tree,  $T_{i,\mathcal{S}}$  ;
7    $\mathcal{Y} \leftarrow \emptyset; \ alg \leftarrow 1$  ;
8    $(\mathcal{Y}, \mathbf{A}) \leftarrow \text{ROW-OP}(\mathbf{A}, \mathcal{S}, i, T_{i,\mathcal{S}}, alg)$  ;
9    $\mathcal{Y}_1.\text{append}(\mathcal{Y}), G' \leftarrow G' \setminus \{i\}$                                 // Remove vertex  $i$  and its edges from  $G'$  ;
10 end
11 Transpose  $\mathbf{A}$  and  $G' \leftarrow G$  ;
12 for columns  $i = 1 \dots, n$  do
13   Repeat steps 3-6 ;
14    $\mathcal{Y} \leftarrow \emptyset; \ alg \leftarrow 2$  ;
15    $(\mathcal{Y}, \mathbf{A}, \mathcal{T}_1) \leftarrow \text{ROW-OP}(\mathbf{A}, \mathcal{S}, i, T_{i,\mathcal{S}}, alg)$  ;
16    $\mathcal{Y}_2.\text{append}(\mathcal{Y})$  ;
17   Initialize an array  $B$  of size  $n$  and  $B[\ell] \leftarrow r$  if  $\ell \in \mathcal{S} \setminus \{i\}$  and  $r$  is the root of the sub-tree in which  $\ell$ 
      was a leaf ;
18    $t \leftarrow |\mathcal{T}_1|$  ;
19   for  $j = 0 \dots t - 1$  do
20      $(r, \ell_1, \dots, \ell_m) \leftarrow \mathcal{T}_1[j]$  ;
21     while  $\exists k$  such that  $\ell_k < r$  do
22        $\ell \leftarrow \ell_k$  ;
23       while  $r > \ell$  do
24          $\mathcal{S} \leftarrow \{r, \ell\}; \ Tr_{r,\mathcal{S}} \leftarrow$  The shortest path between  $r$  and  $\ell$  stored as tree with root  $r$  and leaf
           $\ell$ ;  $\mathcal{Y} \leftarrow \emptyset; \ alg \leftarrow 3$  ;
25          $(\mathcal{Y}, \mathbf{A}) \leftarrow \text{ROW-OP}(\mathbf{A}, \mathcal{S}, r, Tr_{r,\mathcal{S}}, alg)$  ;
26          $\mathcal{Y}_2.\text{append}(\mathcal{Y})$  ;
27          $B[\ell] = B[r], r \leftarrow B[r]$  ;
28       end
29     end
30   end
31    $G' \leftarrow G' \setminus \{i\}$  ;
32 end
33  $\mathcal{Y}'_2 = \mathcal{Y}_2$  with control and target flipped for each CNOT gate ;
34 return  $\mathcal{Y}'_2 \cup \text{reverse}(\mathcal{Y}_1) \cup \mathcal{X}$  as the circuit.

```

---

---

**Algorithm 2:** ROW-OP

---

**Input:** (i) Linear transformation matrix  $\mathbf{A}$ , (ii) Set of terminals  $\mathcal{S}$ , (iii) Pivot node  $c$ , (iv) A minimal Steiner tree approximation  $T_{c,\mathcal{S}}$ , (v)  $alg \in \mathbb{Z}$ .

**Output:** (i) List  $\mathcal{Y}$  of CNOT operations, (ii)  $\mathbf{A}$  (after the row operations), (iii)  $\mathcal{T}_1 = \{(r, \ell_1, \dots, \ell_m) : r \text{ is the root and } \ell_1, \dots, \ell_m \text{ are the leaves in a sub-tree}\}$  if  $alg == 2$ .

```

1  $\mathcal{T} \leftarrow \text{SEPARATE}(T_{c,\mathcal{S}}, c, \mathcal{S}, alg)$  // Separate  $T_{c,\mathcal{S}}$  into a set  $\mathcal{T}$  of sub-trees  $T_{k,\mathcal{S}_k}$  with root  $k \in \mathcal{S}$  and leaves  $\mathcal{S}_k \setminus \{k\} \subset \mathcal{S}$  ;
2  $\mathcal{T}_1 = \{(r, \ell_1, \dots, \ell_m) : r \text{ is the root and } \ell_1, \dots, \ell_m \text{ are the leaves in a sub-tree}\}$  ;
3  $t \leftarrow |\mathcal{T}|$ ;  $\mathcal{Y} \leftarrow \emptyset$  ;
4 for  $i = t - 1, t - 2, \dots, 0$  do // Starting from the last sub-tree do
5   if  $alg \neq 1$  then
6     | (Bottom-Up-1:) Starting from the last layer till layer 1,  $\mathcal{Y}.\text{append}(\text{CNOT}_{uv})$  if  $u$  is a non-root parent node and  $v$  is a child of  $u$  ;
7     | if  $alg \neq 4$  then
8       | |  $\mathbf{A}[v, :] \leftarrow \mathbf{A}[v, :] \oplus \mathbf{A}[u, :]$  ;
9     | end
10   end
11   | (Top-Down1:) Starting from top layer till last layer,  $\mathcal{Y}.\text{append}(\text{CNOT}_{uv})$  if  $u$  is parent of  $v$  ;
12   | if  $alg \neq 4$  then
13     | |  $\mathbf{A}[v, :] \leftarrow \mathbf{A}[v, :] \oplus \mathbf{A}[u, :]$  ;
14   | end
15   | (Bottom-Up-2:) Starting from the last layer till layer 0,  $\mathcal{Y}.\text{append}(\text{CNOT}_{uv})$  if  $u$  is a parent node and  $v$  is a non-leaf child node of  $u$  ;
16   | if  $alg \neq 4$  then
17     | |  $\mathbf{A}[v, :] \leftarrow \mathbf{A}[v, :] \oplus \mathbf{A}[u, :]$  ;
18   | end
19   | if  $alg \neq 1$  then
20     | | (Top-Down-2:) Starting from the second layer till last layer,  $\mathcal{Y}.\text{append}(\text{CNOT}_{uv})$  if  $u$  is a parent node (that is not a child of the root) and  $v$  is a non-leaf child of  $u$  ;
21     | | if  $alg \neq 4$  then
22       | | |  $\mathbf{A}[v, :] \leftarrow \mathbf{A}[v, :] \oplus \mathbf{A}[u, :]$  ;
23     | | end
24   | end
25   | if  $alg == 4$  then
26     | |  $\mathbf{A}[r, :] \leftarrow \mathbf{A}[r, :] \oplus \mathbf{A}[\ell, :]$ , where  $r, \ell$  are the root and leaf of the current sub-tree respectively. ;
27   | end
28 end
29 if  $alg \neq 2$  then
30   | return  $(\mathcal{Y}, \mathbf{A})$  ;
31 else
32   | return  $(\mathcal{Y}, \mathbf{A}, \mathcal{T}_1)$  ;
33 end

```

---

operations performed in steps 11,13 of Algorithm 2 and the 1s at Steiner nodes get cancelled by the operations performed in steps 15, 17 of the same procedure. If in a sub-tree the root node is  $r$  and the leaves are  $\ell_1, \dots, \ell_m$  then the parity at the root node and each Steiner node remains unchanged but the parity at leaf  $\ell_i$  become  $x_{\ell_i} \oplus x_r \bigoplus_{j \in P} x_j$  where  $P$  is the set of Steiner nodes in the path from  $r$  to  $\ell_i$ . The resultant matrix  $\mathbf{A}'$  is in upper triangular form.

Next we transpose  $\mathbf{A}'$ . Our goal is now to convert  $\mathbf{A}'^T$  into upper triangular form without destroying the 0s in the upper-triangle. This in turn implies that for each non-diagonal node  $j$  we want the parity to be  $x'_j \oplus x'_k$ , where  $k < j$  and  $x'_j, x'_k$  are the parities at node  $j$  and  $k$  respectively before the transpose step 11 in Algorithm 1. Similarly as before, we invoke the procedure ROW-OP (Algorithm 2) but this time we include steps 6,8 and 20,22 in it, so that for each sub-tree constructed the parity at root  $r$  and Steiner nodes remain unchanged, but the parity at each leaf node  $\ell$  becomes  $x'_r \oplus x'_\ell$ . Now if  $r > \ell$  then we perform some correction procedures (step 21-29 in Algorithm 1). Note the parity at  $r$  is  $x'_{r_i} \oplus x'_r$  where  $r_i$  is the root of the sub-tree in which  $r$  was a leaf. Then if we invoke ROW-OP with the shortest path from  $r$  to  $\ell$  as a tree, then the parity at  $\ell$  becomes  $x'_{r_i} \oplus x'_\ell$ . Every other parity remains unaffected. If  $r_i > \ell$ , then we again invoke ROW-OP with the shortest path from  $r_i$  to  $\ell$  as a tree. We continue doing this till the parity at  $\ell$  is “corrected” i.e. it becomes  $x'_\ell \oplus x'_k$  for some  $k < \ell$ . We start these correction procedures from the first sub-tree, so we can guarantee that the parity at each node gets corrected as desired.

---

**Algorithm 3: SEPARATE**


---

**Input:** (i) Steiner tree  $T_{c,S}$ , (ii) Pivot  $c$ , (iii) Set of terminals  $S$ . (iv)  $alg \in \mathbb{Z}$ .  
**Output:**  $\mathcal{T} = \{T_{k,S_k} : \text{Edge-disjoint sub-trees with root } k \in S \text{ and leaves } S_k \setminus \{k\} \subset S\}$ .

```

1  $\mathcal{T} \leftarrow \emptyset$ ,  $root \leftarrow c$ ,  $R \leftarrow \{root\}$ ,  $S.delete(c)$  ;
2 while  $S \neq \emptyset$  do
3    $S_{root} \leftarrow \{root\}$ ,  $T_{root,S_{root}} \leftarrow \emptyset$  // Initialize the data-structure to store a sub-tree ;
4   Starting from  $root$ , traverse  $T_{c,S}$  in breadth first search order. Store the vertices and edges in
     $T_{root,S_{root}}$  ;
5   When arriving at a non-leaf terminal  $u$ , then  $S_{root}.append(u)$  and store  $u$  as a leaf in  $T_{root,S_{root}}$ ,
     $S.delete(u)$ ,  $R.append(u)$  ;
6   if  $alg \neq 4$  then
7      $\mathcal{T}.append(T_{root,S_{root}})$  // Store the tree-information depth-wise. ;
8   else
9     for  $u \in S_{root} \setminus \{root\}$  do
10    |  $S_u \leftarrow \{u, root\}$  ;
11    |  $T_{u,S_u} \leftarrow \text{Path from } u \text{ to } root$  // Store the tree as if  $u$  is root and  $root$  is leaf. ;
12    |  $\mathcal{T}.append(T_{u,S_u})$  ;
13  end
14   $R.delete(root)$ ,  $root \leftarrow R[0]$  ;
15 end
16 return  $\mathcal{T}$  ;

```

---

**Remark 3.1**

The use of Steiner trees to take care of connectivity constraints was also done in [34] and [26]. Our procedures are different from both of them. While calling the procedure ROW-OP during the reduction to upper-triangular form (before transpose in step 11 in Algorithm 1) we skipped some steps (steps 6,8 and 20,22 in Algorithm 2) because it was not necessary and this reduced

the CNOT count. We traverse each Steiner tree twice, so the number of CNOT gates required is approximately  $2e$  where  $e$  is the number of edges in the tree. In contrast the algorithm in [34] in this phase consumes approximately  $4e$  CNOT gates. After transposing in step 11 in Algorithm 1 our procedure is markedly different from the approach taken in [34]. Even our “correction procedure” is different from the recursive approach taken in [26] for general graphs. Asymptotically the complexity of LINEAR-TF-SYNTH is similar to the corresponding algorithms in [34] and [26]. There are  $n$  Steiner trees constructed for each of the  $n$  columns. Each Steiner tree approximation will always be of size  $O(n)$ . The number of CNOT gates applied is  $O(n)$ . So overall complexity is  $O(n^2)$ .

An illustration of LINEAR-TF-SYNTH has been shown in Appendix B, using an example given in [34]. We re-synthesize a given linear transformation circuit using 26 CNOTs, while [34] used 43 CNOTs for re-synthesizing the same circuit.

### 3.2 Synthesis of circuits over $\{\text{CNOT}, \text{X}, \text{T}\}$

We consider the circuits implemented with the set of gates  $(\mathcal{G}_{ph})$  generated by  $\{\text{CNOT}, \text{X}, \text{T}\}$ . Since  $\text{S} = \text{T}^2$ ,  $\text{Z} = \text{T}^4$ ,  $\text{T}^\dagger = \text{T}^7$  and  $\text{S}^\dagger = \text{T}^6$ , so  $\mathcal{G}_{ph} = \{\text{CNOT}, \text{X}, \text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{Y}, \text{Z}\}$ . We know from Lemma 2.1 in Section 2.2 that a unitary implemented over  $\{\text{CNOT}, \text{T}\}$  can be characterized by a set  $\mathcal{P} = \{(c, f) : c \in \mathbb{Z}_8 \text{ and } f \in (\mathbb{F}_2^n)^*\}$  and linear reversible output functions  $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  (Equation 6). This actually holds for circuits over  $\{\text{CNOT}, \text{X}, \text{T}\}$ .

Given an  $n$ -qubit circuit over  $\{\text{CNOT}, \text{X}, \text{T}\}$  with input path variables  $x_1, x_2, \dots, x_n$ , we can compute each  $\mathcal{P}$  as follows: For each gate  $U \in \{\text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{Z}, \text{Y}\}$  consider the parity,  $\bigoplus_{j \in \mathcal{S}} x_j \oplus b$  for  $\mathcal{S} \subseteq [n]$ , of the qubit just before  $U$  acts. Here  $b \in \{0, 1\}$  is the *bit variable* that takes the value 1 only after an X or Y gate acts. This is represented by the function  $f$ . The coefficient  $c$  is given by  $\{1, 7, 2, 6, 4, 4, 4\}$  respectively. For  $(c_1, f_1), (c_2, f_2) \in \mathcal{P}$  if  $f_1 = f_2 = f$  then we can merge them into a single pair  $(c_1 + c_2 \bmod 8, f)$ .

The linear reversible output function is  $g : \mathbb{F}_2^n \times \mathbb{F}_2 \rightarrow \mathbb{F}_2^n \times \mathbb{F}_2$  (one of the variables is the bit flip variable  $b$ ). More detail about the matrix representing  $g$  and procedures to synthesize circuits over  $\{\text{CNOT}, \text{X}\}$  that realize  $g$  has been given in Section 3.1.

We follow the approach taken in [1] and [34] while re-synthesizing circuits over  $\{\text{CNOT}, \text{X}, \text{T}\}$ . Both these authors consider a restricted gate set consisting of CNOT and rotation gates  $R_Z$ . Given a phase polynomial set  $\mathcal{P}$  and matrix  $\mathbf{A}$  corresponding to the linear reversible output function  $g$ , they first synthesized a *parity network* (defined below) that realizes the parity terms ( $f$  where  $(c, f) \in \mathcal{P}$ ) in  $\mathcal{P}$ . Then they applied the rotation gates depending on the coefficients ( $c$ ) in  $\mathcal{P}$ . After that they synthesized a circuit such that the overall linear transformation is  $\mathbf{A}$ . While the algorithm in [34] takes care of connectivity constraints, the one in [1] is oblivious to it.

**Definition 3.1 (Parity network).** A parity network for a set  $\mathcal{P} = \{(c, f) : c \in \mathbb{Z}_8 \text{ and } f \in (\mathbb{F}_2^n)^* \times \mathbb{F}_2\}$  is an  $n$ -qubit circuit over  $\{\text{CNOT}, \text{X}\}$  gates in which each *parity* term  $f$  such that  $(c, f) \in \mathcal{P}$  appears at least once.

**Definition 3.2 (Phase polynomial network).** A phase polynomial network for a set  $\mathcal{P} = \{(c, f) : c \in \mathbb{Z}_8 \text{ and } f \in (\mathbb{F}_2^n)^* \times \mathbb{F}_2\}$  is an  $n$ -qubit circuit over  $\{\text{CNOT}, \text{X}, \text{T}\}$  such that for each element  $(c, f) \in \mathcal{P}$  the parity  $f$  appears before a gate in  $\{\text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{Z}, \text{Y}\}$  when  $c \in \{1, 7, 2, 6, 4, 4\}$  respectively.

We now describe our algorithm PHASE-NW-SYNTH (Algorithm 4) that synthesizes a phase polynomial network given by  $\mathcal{P}$ . We construct the parity network matrix  $\mathbf{P}$ , which has  $n$  rows

---

**Algorithm 4: PHASE-NW-SYNTH**


---

**Input:** (i)  $\mathcal{P} \in \{(c, f) : c \in \mathbb{Z}_8 \text{ and } f \in (\mathbb{F}_2^n)^* \times \mathbb{F}_2\}$ , (ii) Connectivity graph  $G$ .

**Output:** A circuit with gates in  $\mathcal{G}_{ph} = \{\text{CNOT}, \text{X}, \text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{Y}, \text{Z}\}$  realizing the phase polynomial network given by  $\mathcal{P}$ .

```

1  $\mathcal{Y}' \leftarrow \emptyset; \quad I \leftarrow [n]; \quad \mathcal{K} \leftarrow \emptyset \quad // \text{Initialize an empty stack } \mathcal{K}.$  ;
2 If  $(c_i, x_i) \in \mathcal{P}$  or  $(c_i, 1 \oplus x_i) \in \mathcal{P}$  for  $i \in [n]$  then  $\mathcal{Y}'.\text{append}(U[i])$  or  $\mathcal{Y}'.\text{append}(X[i]U[i])$  respectively, where  $U[i] \in \mathcal{G}_{ph}$  is determined by  $c_i$ . Then delete these terms from  $\mathcal{P}$ . ;
3 Construct the parity matrix  $\mathbf{P}_{n+2 \times p}$  where  $p = \text{number of terms in } \mathcal{P}$ , the first  $n$  rows of each column is a parity term (without bit flip term),  $n + 1^{\text{th}}$  row stores the bit flip and  $n + 2^{\text{th}}$  row stores the coefficients ;
4  $B \leftarrow \{\mathbf{p}_i : \mathbf{p}_i = [(\mathbf{P}[0 : n - 1, i])^T || i]^T\} \quad // \mathbf{p}_i \text{ is the first } n \text{ rows of } i^{\text{th}} \text{ column of } \mathbf{P}, \text{ appended by } i, \text{ the column index.}$  ;
5 if  $B \neq \emptyset$  then
6   |  $\mathcal{K}.\text{push}(B, I, \epsilon)$  ;
7 end
8 while  $\mathcal{K} \neq \emptyset$  do
9   |  $(B, I, i) \leftarrow \mathcal{K}.\text{pop}()$  ;
10  | if  $i \in \mathbb{N}$  then
11    |   |  $\mathcal{S}' \leftarrow \{k \in [n] : k \neq i \text{ and } p_k = 1 \quad \forall \mathbf{p} \in B\}$  ;
12    |   | if  $\mathcal{S}' \neq \emptyset$  then
13      |     |   |  $\mathcal{S} = \mathcal{S}' \cup \{i\}$  ;  $alg \leftarrow 4$  ;
14      |     |   | Find a minimum Steiner tree approximation with connectivity graph  $G$  and terminals  $\mathcal{S}$ . Let  $i$  be the root of this tree,  $T_{i,\mathcal{S}}$  ;
15      |     |   |  $\mathbf{A} = \text{Matrix with columns } \mathbf{p} \in B' \text{ such that } (B', I', i') \in \mathcal{K} \cup (B, I, i)$  ;
16      |     |   |  $\mathcal{Y} \leftarrow \emptyset$  ;
17      |     |   |  $(\mathcal{Y}, \mathbf{A}) \leftarrow \text{ROW-OP}(\mathbf{A}, \mathcal{S}, i, T_{i,\mathcal{S}}, 4)$  ;
18      |     |   |  $\mathcal{Y}'.\text{append}(\mathcal{Y})$  ;
19      |     |   | if  $\exists \mathbf{p} \in B'$  where  $(B', I', i') \in \mathcal{K} \cup (B, I, i)$  such that  $p_k = 0$  for  $k \in [n]$  and  $k \neq i$  then
20        |       | At the place in the circuit where the parity given by  $p_n^{\text{th}}$  column of  $\mathbf{P}$  is realized, place
21        |       |   | (append in  $\mathcal{Y}'$ )  $XU$  or  $U$  (accordingly) ;
22        |       |   |  $B'.$ delete( $\mathbf{p}$ ) ;
23        |     end
24      end
25    end
26  end
27  |  $j \leftarrow \arg \max_{j \in I} \max_{x \in \mathbb{F}_2} |\{\mathbf{p} \in B : p_j = x\}|$  ;
28  |  $B_0 \leftarrow \{\mathbf{p} \in B : p_j = 0\}; \quad B_1 \leftarrow \{\mathbf{p} \in B : p_j = 1\}$  ;
29  | if  $B_1 \neq \emptyset$  then
30    |   | if  $i = \epsilon$  then
31      |     |   |  $\mathcal{K}.\text{push}(B_1, I \setminus \{j\}, j)$  ;
32    |   | else
33      |     |   |  $\mathcal{K}.\text{push}(B_1, I \setminus \{j\}, i)$  ;
34    |   end
35  | if  $B_0 \neq \emptyset$  then
36    |   |  $\mathcal{K}.\text{push}(B_0, I \setminus \{j\}, i)$  ;
37 end
38 return  $\mathcal{Y}'$  ;

```

---

corresponding to each qubit and where each column corresponds to a parity term  $f$  in  $\mathcal{P}$ . Similar to [1], the optimization procedure to synthesize the parity network represented by  $\mathbf{P}$  is inspired by *Gray codes* [15], which cycle through the set of  $n$ -bit strings using the exact minimal number of bit flips. Given a set  $B$  of binary strings (step 4), we synthesize a parity network for  $B$  by repeatedly choosing an index  $j$  (step 25) to expand and then effectively recurring on the co-factors  $B_0$  and  $B_1$  (step 26), consisting of the strings  $\mathbf{p} \in B$  with  $p_j = 0$  or 1 respectively. As a subset  $B$  is recursively expanded, CNOT gates are applied so that a designated *target* qubit  $i$  contains the partial parity  $\bigoplus_{k \in \mathcal{S}'} x_k$  where  $\mathcal{S}'$  is the set of qubits (or row indices) such that  $p_k = 1$  ( $k \neq i$ ) for all  $\mathbf{p} \in B$  (step 11). Whenever a column has a single 1, it implies that the corresponding parity has been realized. So we can remove these columns from the set  $B'$  of “remaining parities” (steps 19-22). At this step we can place the gate  $X$  if parity realized on circuit is  $1 \oplus f$  for some  $(c, f) \in \mathcal{P}$ . We can also place a gate in  $\{T, T^\dagger, S, S^\dagger, Z, Y\}$  corresponding to the value of the coefficient  $c$ .

To incorporate connectivity constraints we find a minimal Steiner tree  $T_{i,\mathcal{S}}$  with connectivity graph  $G$  and terminals  $\mathcal{S} = \mathcal{S}' \cup \{i\}$  (step 14). We call the procedure ROW-OP (Algorithm 2) with the matrix  $\mathbf{A}$  such that its columns are the set of unrealized parities 15. ROW-OP calls the sub-routine SEPARATE 3 which as before separates  $T_{i,\mathcal{S}}$  into edge-disjoint sub-trees such that in each tree the root and leaves belong to set of terminals  $\mathcal{S}$ . However, unlike the previous methods, this time each sub-tree with multiple leaves are further sub-divided such that each tree has a single leaf. Each such tree is stored in reverse depth-first order such that the leaf becomes root and vice-versa (steps 9-11 in Algorithm 3). Now when we perform steps 4-27 of Algorithm 2 then for each sub-tree the parity at root is  $x_r \oplus x_\ell$  where  $r, \ell$  are the root and leaf of the sub-tree respectively (before flipping). Now since we process the trees from last sub-tree to first, so the net parity at node (or qubit  $i$ ) is  $\bigoplus_{k \in \mathcal{S}'} x_k$ . To maintain the invariant that the remaining parities are expressed over the current state of the qubits, we modify the matrix  $\mathbf{A}$  as given in step 26 of Algorithm 2.

### Remark 3.2

In [34] an algorithm to synthesize parity networks over  $\{\text{CNOT}, R_z\}$  was described and a somewhat similar scheme was sketched in [26]. Both used Steiner trees and the sum-over-path formulation of such circuits. Our algorithm is significantly different from both, especially considering the way we assigned CNOT gates according to the constructed Steiner trees.

An illustration of PHASE-NW-SYNTH has been given in Appendix C.

## 4 Synthesis of circuits over $\{\text{CNOT}, X, T, H\}$ gates

Finally in this section we are in a position to describe our re-synthesis algorithms that takes as input a circuit  $\mathcal{C}_I$  over a universal fault-tolerant gate set  $\mathcal{G}_{univ} = \{\text{CNOT}, T, T^\dagger, S, S^\dagger, X, Y, Z, H\}$  and it outputs a circuit  $\mathcal{C}_O$  with gates in the same set, but the position of the CNOT gates are restricted by some connectivity constraints imposed by an input connectivity graph  $G$ .

The basic format of our re-synthesis algorithms include *slicing* the given circuit and *building* the sliced portions. We partition the given circuit at the position of the  $H$  gates and then sequentially re-synthesize sub-circuits in each portion such that the transformation within each portion and the overall circuit transformation remains unchanged. We investigate two methods of slicing - the first one is a simple *slice-and-build*, where we partition the input circuit according to the position of the  $H$  gate and the second one is motivated by the Tpar algorithm given in [3], where the phase

polynomial terms are partitioned. Unlike Tpar we are not interested in reducing the T-depth of the input circuit. So we partition the phase polynomial terms depending only on the path variables, which indicate the parities that can be synthesized before or after a certain H gate.

#### 4.1 Simply slice-and-build

---

##### Algorithm 5: CNOT-OPT-A

---

**Input:** (i) Circuit  $\mathcal{C}_I$  with  $\{\text{CNOT}, \text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{X}, \text{Y}, \text{Z}, \text{H}\}$  gates, (ii) Connectivity graph  $G$ .  
**Output:** Circuit  $\mathcal{C}_O$  with CNOT gates respecting connectivity constraints imposed by  $G$ .

```

1  $\mathcal{C}_O \leftarrow \emptyset; \quad i = -1; \quad \text{gate} = \text{START} ;$ 
2 while  $\text{gate} \neq \text{EOF}$  do
3    $i \leftarrow i + 1; \quad \text{gate} = \mathcal{C}_O[i]; \quad Q = (x_1, x_2, \dots, x_n); \quad \mathcal{P} \leftarrow \emptyset ;$ 
4   while  $\text{gate} \neq \text{H}$  or  $\text{gate} \neq \text{EOF}$  do
5     Update  $Q$  and  $\mathcal{P}$  according to the rules described in Section 4.1 ;
6      $i \leftarrow i + 1; \quad \text{gate} = \mathcal{C}_O[i] ;$ 
7   end
8    $\mathcal{C}_{ph}, \mathcal{C}_{lin} \leftarrow \emptyset ;$ 
9    $\mathcal{C}_{ph} \leftarrow \text{PHASE-NW-SYNTH}(\mathcal{P}, G) ;$ 
10   $Q_{ph} \leftarrow \text{state of the qubits after } \mathcal{C}_{ph} ;$ 
11   $\mathbf{A} \leftarrow \text{linear transformation mapping } Q_{ph} \text{ to } Q ;$ 
12   $\mathcal{C}_{lin} \leftarrow \text{LINEAR-TF-SYNTH}(\mathbf{A}, G) ;$ 
13   $\mathcal{C}_O.append(\mathcal{C}_{ph}, \mathcal{C}_{lin}, \text{H}[k]) \quad // k \text{ is the position of H} ;$ 
14 end
15 return  $\mathcal{C}_O ;$ 

```

---

In our first algorithm CNOT-OPT-A (Algorithm 5) we first partition the given circuit at the position of H gates. Within each partition we initialize the state of the qubits  $Q$  by the path variables  $(x_1, x_2, \dots, x_n)$  and the phase polynomial set  $\mathcal{P}$  as empty set (step 3). Then with the application of each gate  $U_i \in \mathcal{G}_{univ}$  or  $U_{(ij)} \in \mathcal{G}_{univ}$ , we update  $Q$  and  $\mathcal{P}$  (step 4-step 6) by the function  $\tilde{U}_i : \langle \mathcal{P}, Q \rangle \rightarrow \langle \mathcal{P}, Q \rangle$  as follows.

$$\begin{aligned}
\widetilde{\text{X}}_i \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P}, (q_1, \dots, q_{i-1}, 1 \oplus q_i, \dots, q_n) \rangle ; \\
\widetilde{\text{CNOT}}_{(i,j)} \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P}, (q_1, \dots, q_{j-1}, q_i \oplus q_j, \dots, q_n) \rangle ; \\
\widetilde{\text{S}}_i \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P} \uplus \{(2, q_i)\}, Q \rangle ; & \widetilde{\text{S}}_i^\dagger \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P} \uplus \{(6, q_i)\}, Q \rangle ; \\
\widetilde{\text{T}}_i \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P} \uplus \{(1, q_i)\}, Q \rangle ; & \widetilde{\text{T}}_i^\dagger \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P} \uplus \{(7, q_i)\}, Q \rangle ; \\
\widetilde{\text{Z}}_i \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P} \uplus \{(4, q_i)\}, Q \rangle ; \\
\widetilde{\text{Y}}_i \langle \mathcal{P}, Q \rangle &= \langle \mathcal{P} \uplus \{(4, q_i)\}, (q_1, \dots, q_{i-1}, 1 \oplus q_i, \dots, q_n) \rangle ;
\end{aligned}$$

In the above set of equations, for two sets  $\mathcal{P}'$  and  $\mathcal{P}''$ ,  $\mathcal{P}' \uplus \mathcal{P}'' = \{(c, f) : (c_1, f) \in \mathcal{P}', (c_2, f) \in \mathcal{P}'', c = c_1 + c_2 \pmod{8}\}$ . Here we assume that if  $\exists f$  such that  $(c, f) \notin \mathcal{P}$  for any  $c = \{1, \dots, 7\}$  and any set  $\mathcal{P}$ , then we say  $(0, f) \in \mathcal{P}$ .

Then we synthesize the phase polynomial network ( $\mathcal{C}_{ph}$ ) for  $\mathcal{P}$  (step 9) by invoking the procedure PHASE-NW-SYNTH (Algorithm 4). We calculate the linear transformation  $\mathbf{A}$  (step 11) mapping  $Q_{ph}$  (state of the qubits after  $\mathcal{C}_{ph}$ ) to  $Q$ , which after steps 4-6 stores the state of the qubits at the end of the present slice. We synthesize the circuit  $\mathcal{C}_{lin}$  for  $\mathbf{A}$  (step 12) using the procedure

LINEAR-TF-SYNTH (Algorithm 1). We append the gates from  $\mathcal{C}_{ph}, \mathcal{C}_{lin}$  followed by the H gate (step 13). Then we repeat the same steps for the next slice (till the next H gate or the end of the given circuit).

---

**Algorithm 6: CNOT-OPT-B**


---

**Input:** (i) Circuit  $\mathcal{C}_I$  with  $\{\text{CNOT}, \text{T}, \text{T}^\dagger, \text{S}, \text{S}^\dagger, \text{X}, \text{Y}, \text{Z}, \text{H}\}$  gates, (ii) Connectivity graph  $G$ .  
**Output:** Circuit  $\mathcal{C}_O$  with CNOT gates respecting connectivity constraints imposed by  $G$ .

```

1  $\mathcal{C}_O \leftarrow \emptyset$ ;
2 From  $\mathcal{C}_I$  calculate  $\mathcal{D} = \langle \mathcal{P}, \mathcal{Q}, \mathcal{H} \rangle$ ;  $k \leftarrow |\mathcal{H}|$ .                                // Described in Section 4 ;
3  $Q_{init} = (x_1, x_2, \dots, x_n)$ ;  $Q_{out} = Q$  ;
4 for  $1 \leq i \leq k$  do
5    $h \leftarrow \mathcal{H}_i$ ;  $\mathcal{C}_{ph} \leftarrow \emptyset$ ;  $\mathcal{C}_{lin} \leftarrow \emptyset$  ;
6    $\mathcal{P}' \leftarrow \{(c, f) \in \mathcal{P} : f \in \text{span}(h.Q_I) \text{ but } f \notin \text{span}(h.Q_O)\}$  ;
7   if  $\mathcal{P}' \neq \emptyset$  then
8      $\mathcal{P}.delete(\mathcal{P}')$  ;
9      $\mathcal{P}_{Q_{init}} \leftarrow \{(c, f) \in \mathcal{P}' \text{ in the basis } Q_{init}\}$  ;
10     $\mathcal{C}_{ph} \leftarrow \text{PHASE-NW-SYNTH}(\mathcal{P}_{Q_{init}}, G)$  ;
11     $Q_{ph} \leftarrow \text{state of the qubits after } \mathcal{C}_{ph}$  ;
12     $\mathbf{A} \leftarrow \text{linear transformation mapping } Q_{ph} \text{ to } h.Q_I$  ;
13     $\mathcal{C}_{lin} \leftarrow \text{LINEAR-TF-SYNTH}(\mathbf{A}, G)$  ;
14  end
15   $Q_{init} \leftarrow h.Q_O$  ;
16   $\mathcal{C}_O.append(\mathcal{C}_{ph}, \mathcal{C}_{lin}, \mathbf{H}[k])$  where  $k = h.Pos$  ;
17 end
18  $\mathcal{C}_{ph} \leftarrow \emptyset$ ;  $\mathcal{C}_{lin} \leftarrow \emptyset$  ;
19 if  $\mathcal{P}' \neq \emptyset$  then
20    $\mathcal{P}_{Q_{init}} = \{(c, f) \in \mathcal{P} \text{ in the basis } Q_{init}\}$  ;
21    $\mathcal{C}_{ph} \leftarrow \text{PHASE-NW-SYNTH}(\mathcal{P}_{Q_{init}}, G)$  ;
22    $Q_{ph} \leftarrow \text{state of the qubits after } \mathcal{C}_{ph}$  ;
23 else
24    $Q_{ph} \leftarrow Q_{init}$  ;
25 end
26  $\mathbf{A} \leftarrow \text{linear transformation mapping } Q_{ph} \text{ to } Q_{out}$  ;
27  $\mathcal{C}_{lin} \leftarrow \text{LINEAR-TF-SYNTH}(\mathbf{A}, G)$  ;
28  $\mathcal{C}_O.append(\mathcal{C}_{ph}, \mathcal{C}_{lin})$  ;
29 return  $\mathcal{C}_O$  ;

```

---

### Remark 4.1

The intuition behind this kind of slice-and-build is as follows. Suppose the number of CNOT in the input circuit is  $N_1$ .

Consider a simple method where we simply apply the SWAP-template on each CNOT gate. Suppose we require  $N'_1$  number of CNOT gates.

Now consider a second method. Between two H gates (as well as the portion before the first and the portion after the last H gate) there is a phase polynomial network. If we apply the algorithm of [1] to each such portion then we expect to get reduction in overall CNOT count from  $N_1$  to  $N_2$ , say. Since [1] is not connectivity-constraint-aware, so we apply the SWAP template on each CNOT obtained after applying [1]. Let the number of CNOTs required be  $N'_2$  and we can expect  $N'_2 < N'_1$ . We are saying ‘‘expect’’ because [1] does not have a proof that it will reduce the CNOT-count in all instances. The result is empirical indicating a reduction in many cases.

Architecture	#Qubits	Initial Count	SWAP-template Overhead	CNOT-OPT-A		CNOT-OPT-B		Qiskit Overhead
				Overhead	Time	Overhead	Time	
9q-square	9	3	560%	0.00%	0.184s	343%	0.105s	310%
		5	612%	146%	0.146s	400%	0.128s	300%
		10	594%	105%	0.167s	426%	0.119s	303%
		20	546%	176%	0.2s	488%	0.158s	265.50%
		30	596%	184.67%	0.233s	649%	0.185s	310%
16q-square	16	4	1050%	238%	0.23s	768%	0.12s	562.50%
		8	840%	146.25%	0.27s	660%	0.137s	461.25%
		16	817.50%	158.13%	0.43s	864%	0.225s	470.63%
		32	853%	340.63%	0.41s	1213%	0.29s	493.13%
		64	892.50%	220.78%	0.49s	1259%	0.65s	476.25%
		128	858.75%	210.63%	0.57s	1156%	1.144s	475.31%
		256	897.42%	237.5%	0.72s	1306%	1.85s	497.46%
rigetti-16q-aspen	16	4	1680%	355%	0.23s	1278%	0.115s	750%
		8	1740%	253%	0.396s	1313%	0.135s	738.75%
		16	1619.90%	351%	0.47s	1304%	0.162s	701.25%
		32	1794%	469.48%	0.48s	1852%	0.375s	732.19%
		64	1755%	399%	0.66s	1900%	0.71s	728.91%
		128	1760.63%	368.13%	0.58s	1953%	1.37s	731.02%
		256	1757.11%	410.9%	0.61s	1982%	1.68s	725.74%
ibm-qx5	16	4	1260%	173%	0.38s	988%	0.108s	690%
		8	1035%	295%	0.36s	1065%	0.126s	712.50%
		16	1042.50%	283%	0.41s	1226%	0.47s	710.63%
		32	1179.38%	398.44%	0.42s	1677%	0.68s	670.31%
		64	1130.63%	339.06%	0.45s	1733%	0.7s	646.88%
		128	1110.94%	344.69%	0.575s	1675%	1.15s	689.30%
		256	1141.17%	379.88%	0.73s	1792%	1.58s	678.52%
ibm-q20-tokyo	20	4	525%	128%	0.186s	418%	0.4s	435%
		8	555%	275%	0.295s	690%	0.37s	506.25%
		16	570%	88%	0.37s	663%	0.41s	472.50%
		32	500.63%	154.38%	0.55s	972%	0.8s	420%
		64	542.81%	136.88%	0.54s	1084%	0.82s	463.59%
		128	539.53%	141.02%	0.645s	1028%	1.29s	468.05%
		256	534.61%	125.27%	0.72s	1030%	2.085s	457.50%

Table 1: Performance of CNOT-OPT-A and CNOT-OPT-B for random circuits. The overhead or increase in CNOT-count has been compared to the overhead obtained by using SWAP-template and Qiskit transpiler.

Architecture	#Qubits	Benchmark	SWAP-template Overhead	CNOT-OPT-A		CNOT-OPT-B		Qiskit Overhead
				Overhead	Time	Overhead	Time	
9q-square	9	barenco-tof-5	457.14%	245.24%	0.365s	140.48%	0.52s	232.14%
		grover-5	685.71%	116.67%	0.502s	105.36%	0.84s	219.64%
		mod-mult-55	752.73%	321.82%	0.31s	203.64%	0.26s	256.36%
		tof-5	465.31%	140.82%	0.27s	138.78%	0.24s	226.53%
16q-square	16	hw10	977.95%	-63%	8.77s	-57.67%	7.25s	284.76%
rigetti-16q-aspen	16		1508.63%	-36.13%	8.8s	-34.29%	6.64s	356.70%
ibm-qx5	16		1099.84%	-54.32%	6.18s	-50.75%	8.61s	321.71%
ibm-q20-tokyo	20	ham15-high	571.44%	-52.52%	0.72s	-63.21%	0.66s	242.76%
		hw12	619.42%	-77.58%	177.23s	-74.92%	231.14s	277.82%

Table 2: Performance of CNOT-OPT-A and CNOT-OPT-B for benchmark circuits. The overhead or increase in CNOT-count has been compared to the overhead obtained by using SWAP-template and Qiskit transpiler.

Now consider a third method where we apply our connectivity-constraint-aware algorithm in each phase polynomial network. This keeps the CNOT-count reduction technique of [1], while working with multiple rows at a time. To be precise, [1] reduces one particular row of a group of columns at a time. By “reduce” we mean flipping 1 to 0. We reduce multiple such rows at a time. Using Steiner trees we find the shortest path that connects these nodes in the graph. Since these two things are done together, so we can expect a further reduction in CNOT-count compared to method 1 and 2. Thus if  $N'_3$  is the CNOT-count obtained using our algorithm, we can expect  $N'_3 < N'_2 < N'_1$ . Again, we say “expect” since there is no concrete mathematical proof.

## 4.2 A second type of slice-and-build

In this section we describe another way of slicing the given circuit, as described in procedure CNOT-OPT-B (Algorithm 6). Unlike CNOT-OPT-A, here we first compute some necessary information about the whole circuit and then between two H gates we try to synthesize a circuit that computes part of the information. Similar to CNOT-OPT-A the transformations between two H gates as well as the overall transformation remain unchanged. That is, given  $\mathcal{C}_I$ , we first compute a triple  $\mathcal{D} = \langle \mathcal{P}, Q, \mathcal{H} \rangle$ , where  $\mathcal{P}$  is the phase polynomial set,  $Q = (q_1, q_2, \dots, q_n)$  represents the state of each qubit given as a function of the path variables and the bit flip variable  $b \in \{0, 1\}$ , and  $\mathcal{H}$  is an array of structures where the  $i^{th}$  structure stores the state of the qubits before and after the application of the  $i^{th}$  H gate. The initial state of the qubits is  $Q = (x_1, x_2, \dots, x_n)$  (i.e.  $q_i = x_i \quad \forall i$ ). Both  $\mathcal{P}$  and  $\mathcal{H}$  are initialized as empty sets. With the application of each gate  $U_i \in \mathcal{G}_{univ}$  or  $U_{(i,j)} \in \mathcal{G}_{univ}$  (subscripts denote the qubit on which the gate acts) the triple  $\mathcal{D}$  gets updated by a function  $\widetilde{U}_i' : \mathcal{D} \rightarrow \mathcal{D}$ . Except for the H gate, this function is similar to the function  $\widetilde{U}_i$  defined in Section 4.1. The array  $\mathcal{H}$  remains unchanged after the application of  $\widetilde{U}_i'$  for each gate except H. For the H gate the function is defined as follows.

$$\widetilde{H}_i \langle \mathcal{P}, Q, \mathcal{H} \rangle = \langle \mathcal{P}, Q', \mathcal{H}' \rangle \text{ where } Q' = (q_1, \dots, q_{i-1}, x_{n+j+1}, \dots, q_n) \text{ and } \mathcal{H}' = \mathcal{H} \cup \{h_{j+1}\} \\ \text{such that } h_{j+1}.Pos = i, \quad h_{j+1}.Q_I = Q, \quad h_{j+1}.Q_O = Q' \quad [\text{Here } |\mathcal{H}| = j.]$$

$h_{j+1}.Pos$  stores the qubit (which in the above equation is the  $i^{th}$  one) on which the  $(j+1)^{th}$  H gate is applied.  $h_{j+1}.Q_I$  and  $h_{j+1}.Q_O$  stores the state of the qubits before and after the application of

the  $(j+1)^{th}$  H gate respectively. We have introduced new path variables after application of each H gate. We actually slice the sets  $\mathcal{P}, Q$  and  $\mathcal{H}$  according to some conditions and synthesize circuits according to these slices.

For each  $h \in \mathcal{H}$  we calculate the set  $\mathcal{P}' = \{(c, f) \in \mathcal{P} : f \in \text{span}(h.Q_I) \text{ but } f \notin \text{span}(h.Q_O)\} \subseteq \mathcal{P}$  of parity terms that become uncomputable after placement of H at qubit  $h.Pos$  (step 6 in Algorithm 6). We express these parities in the basis given by the state of the qubits at the beginning of the current time slice, which is  $Q_{init} = (x_1, \dots, x_n)$  if  $h$  is the first Hadamard gate, else it is  $h'.Q_O$ , the state of the qubits after the previous H gate (step 9). We then calculate the phase polynomial network  $(\mathcal{C}_{ph})$  for the set  $\mathcal{P}_{Q_{init}}$  ( $\mathcal{P}'$  in the new basis i.e. parity terms in  $\mathcal{P}'$  as function of  $Q_{init}$ ) by invoking the procedure PHASE-NW-SYNTH (Algorithm 4). Let  $Q_{ph}$  is the state of the qubits after  $\mathcal{C}_{ph}$  and  $\mathbf{A}$  is the linear transformation mapping  $Q_{ph}$  to  $h.Q_I$ . To realize this transformation in this portion of the circuit we call the procedure LINEAR-TF-SYNTH (Algorithm 1). We append  $(\mathcal{C}_{ph}, \mathcal{C}_{lin}, H[k])$  to the set of circuit gates, where  $\mathcal{C}_{lin}$  is the circuit returned by LINEAR-TF-SYNTH and  $k = h.Pos$ .

After we process all the partitions till the last Hadamard gate we ensure that the complete phase polynomial set  $\mathcal{P}$  has been synthesized and the overall linear transformation of the output circuit maps  $(x_1, x_2, \dots, x_n)$  to  $Q_{out}$ , the final output of the circuit (which was calculated at the beginning while calculating  $\mathcal{D}$ ). For this we first synthesize the phase polynomial network  $\mathcal{C}_{ph}$  of any residual parity terms (step 21 in Algorithm 6). Then we calculate the residual transformation  $\mathbf{A}$  (step 26) that maps  $Q_{ph}$ , state of the qubits after  $\mathcal{C}_{ph}$ , to  $Q_{out}$ . And synthesize the circuit  $\mathcal{C}_{lin}$  (step 27) for  $\mathbf{A}$ .

### 4.3 Implementation and results

We have considered the connectivity constraints imposed by some popular architectures such as 9-qubit square grid (Figure 1), 16-qubit square grid, Rigetti 16-qubit Aspen, 16-qubit IBM QX5 and 20-qubit IBM Tokyo (Figure 2). We have worked with some benchmark circuits (Table 2) and some randomly generated circuits on 9, 16 and 20 qubits (Figure 1). The 9-qubit random input circuits have CNOT-count 3, 5, 10, 20 or 30, while both the 16 and 20-qubit random input circuits have CNOT-count 4, 8, 16, 32, 64, 128 or 256. For each of these groups we generated 10 random circuits. We have compared the CNOT-count overhead obtained by using SWAP-template (Figure 1) and Qiskit transpiler with the CNOT-count obtained from procedures CNOT-OPT-A (Algorithm 5) and CNOT-OPT-B (Algorithm 6). By overhead we mean the percentage increase in CNOT-count after taking into consideration connectivity constraints. The results for benchmark circuits and the random circuits have been tabulated in Table 2 and 1 respectively. All the simulations have been done in Java on a 3.1 GHz Dual-Core Intel Core i7 machine with 8GB RAM and running MacOS Catalina 10.15.2. We find that both our algorithms perform quite well in the case of benchmark circuits. CNOT-OPT-A performs much better than the other algorithms in the case of random circuits.

## 5 Conclusion

While implementing a quantum algorithm on an actual hardware, one needs to consider the different constraints imposed by the underlying physical architecture. One such constraint is the qubit connectivity, which is more concerning for multi-qubit gates such as CNOT. In a universal fault-tolerant

gate set such as CNOT+T, although the T-gate is the most costly to implement fault-tolerantly, the CNOT-count is also important, especially in the NISQ era. In this work we have considered the problem of re-synthesizing Clifford+T circuits with reduced CNOT-count compared to the SWAP-template, while respecting the connectivity constraint. Broadly, we have taken recourse to a slice-and-build approach, where we slice or partition the input circuit and re-synthesize the slices with algorithms that use Steiner trees to place the CNOT gates. We have simulated benchmarks as well as random circuits on popular architectures such as 9-qubit square grid, 16-qubit square grid, Rigetti 16-qubit Aspen, 16-qubit IBM QX5 and 20-qubit IBM Tokyo. Our results show that for both benchmarks and random circuits the simpler way of slicing the circuit (and not the phase polynomial) results in much less overhead in terms of increase in CNOT-count, compared to the overhead obtained by using SWAP-template and Qiskit transpiler.

## Acknowledgement

This work was supported in part by Canada’s NSERC. IQC and the Perimeter Institute (PI) are supported in part by the Government of Canada and Province of Ontario (PI). A significant part of this work was done while S.M.Li was a student at the Department of Mathematics and Statistics, Dalhousie University, Halifax NS, Canada and was an under-graduate research intern at IQC.

## Author contributions

The ideas were given by P.Mukhopadhyay. The implementations were done by S.M.Li and J.Huang. All the authors contributed in preparation of the manuscript.

## Data availability

The results obtained in this paper are available in a Github repository at <https://github.com/SarahMLi/cnotcount>.

## Code availability

The code is available from the corresponding author on reasonable request.

## Competing interests

Michele Mosca is co-founder of softwareQ Inc. and has filed a provisional patent application for this work. P.Mukhopadhyay and V.Gheorghiu are co-inventors.

## References

- [1] Matthew Amy, Parsiad Azimzadeh, and Michele Mosca. On the controlled-not complexity of controlled-not–phase circuits. *Quantum Science and Technology*, 4(1):015002, 2018.

- [2] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004.
- [3] Matthew Amy, Dmitri Maslov, and Michele Mosca. Polynomial-time t-depth optimization of clifford+ t circuits via matroid partitioning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(10):1476–1489, 2014.
- [4] Debjyoti Bhattacharjee and Anupam Chattopadhyay. Depth-optimal quantum circuit placement for arbitrary topologies. *arXiv preprint arXiv:1703.08540*, 2017.
- [5] Jarosław Byrka, Fabrizio Grandoni, Thomas Rothvoss, and Laura Sanit  . Steiner tree approximation via iterative randomized rounding. *Journal of the ACM (JACM)*, 60(1):1–33, 2013.
- [6] CJ Ballance, TP Harty, NM Linke, MA Sepiol, and DM Lucas. High-fidelity quantum logic gates using trapped-ion hyperfine qubits. *Physical review letters*, 117(6):060504, 2016.
- [7] Stephen Brierley. Efficient implementation of quantum circuits with limited qubit interactions. *Quantum Information & Computation*, 17(13-14):1096–1104, 2017.
- [8] Joseph W Britton, Brian C Sawyer, Adam C Keith, C-C Joseph Wang, James K Freericks, Hermann Uys, Michael J Biercuk, and John J Bollinger. Engineered two-dimensional ising interactions in a trapped-ion quantum simulator with hundreds of spins. *Nature*, 484(7395):489, 2012.
- [9] Alexander Cowtan, Silas Dilkes, Ross Duncan, Alexandre Krajenbrink, Will Simmons, and Seyon Sivarajah. On the qubit routing problem. *arXiv preprint arXiv:1902.08091*, 2019.
- [10] Amlan Chakrabarti, Susmita Sur-Kolay, and Ayan Chaudhury. Linear nearest neighbor synthesis of reversible circuits by graph partitioning. *arXiv preprint arXiv:1112.0564*, 2011.
- [11] Timoth   Goubault de Brugi  re, Marc Baboulin, Beno  t Valiron, Simon Martiel, and Cyril Allouche. Quantum cnot circuits synthesis for nisq architectures using the syndrome decoding problem. In *International Conference on Reversible Computation*, pages 189–205. Springer, 2020.
- [12] Christopher M Dawson, Andrew P Hines, Duncan Mortimer, Henry L Haselgrove, Michael A Nielsen, and Tobias J Osborne. Quantum computing and polynomial equations over the finite field  $\mathbb{Z}_2$ . *Quantum Information & Computation*, 5(2):102–112, 2005.
- [13] Davide Ferrari and Michele Amoretti. Demonstration of envariance and parity learning on the ibm 16 qubit processor. *arXiv preprint arXiv:1801.02363*, 2018.
- [14] Richard P Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21(6/7), 1982.
- [15] Gray Frank. Pulse code communication, March 17 1953. US Patent 2,632,058.
- [16] Daniel Gottesman. The heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006*, 1998.

- [17] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, Jul 1997.
- [18] John P Gaebler, Ting Rei Tan, Y Lin, Y Wan, R Bowler, Adam C Keith, S Glancy, K Coakley, E Knill, D Leibfried, et al. High-fidelity universal gate set for be 9+ ion qubits. *Physical review letters*, 117(6):060505, 2016.
- [19] Yuichi Hirata, Masaki Nakanishi, Shigeru Yamashita, and Yasuhiko Nakashima. An efficient conversion of quantum circuits to a linear nearest neighbor architecture. *Quantum Information and Computation*, 11(1):142, 2011.
- [20] WK Hensinger, S Olmschenk, D Stick, D Hucul, M Yeo, M Acton, L Deslauriers, C Monroe, and J Rabchuk. T-junction ion trap array for two-dimensional ion shuttling, storage, and manipulation. *Applied Physics Letters*, 88(3):034101, 2006.
- [21] Frank K Hwang and Dana S Richards. Steiner tree problems. *Networks*, 22(1):55–89, 1992.
- [22] Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita. Transformation rules for designing cnot-based quantum circuits. In *Proceedings of the 39th annual Design Automation Conference*, pages 419–424, 2002.
- [23] Toshinari Itoko, Rudy Raymond, Takashi Imamichi, Atsushi Matsuo, and Andrew W Cross. Quantum circuit compilers using gate commutation rules. In *Proceedings of the 24th Asia and South Pacific Design Automation Conference*, pages 191–196, 2019.
- [24] Toshinari Itoko, Rudy Raymond, Takashi Imamichi, and Atsushi Matsuo. Optimization of quantum circuit mapping using gate transformation and commutation. *Integration*, 70:43–50, 2020.
- [25] Richard M Karp. Reducibility among combinatorial problems. In *Complexity of computer computations*, pages 85–103. Springer, 1972.
- [26] Aleks Kissinger and Arianne Meijer-van de Griend. Cnot circuit extraction for topologically-constrained quantum memories. *arXiv preprint arXiv:1904.00633*, 2019.
- [27] Dax E Koh, Mark D Penney, and Robert W Spekkens. Computing quopit clifford circuit amplitudes by the sum-over-paths technique. *Quantum Information & Computation*, 17(13-14):1081–1095, 2017.
- [28] Joseph B Kruskal. On the shortest spanning subtree of a graph and the traveling salesman problem. *Proceedings of the American Mathematical society*, 7(1):48–50, 1956.
- [29] Gushu Li, Yufei Ding, and Yuan Xie. Tackling the qubit mapping problem for nisq-era quantum devices. In *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 1001–1014, 2019.
- [30] Aaron Lye, Robert Wille, and Rolf Drechsler. Determining the minimal number of swap gates for multi-dimensional nearest neighbor quantum circuits. In *The 20th Asia and South Pacific Design Automation Conference*, pages 178–183. IEEE, 2015.

[31] Prakash Murali, Ali Javadi-Abhari, Frederic T Chong, and Margaret Martonosi. Formal constraint-based compilation for noisy intermediate-scale quantum systems. *Microprocessors and Microsystems*, 66:102–112, 2019.

[32] Ashley Montanaro. Quantum circuits and low-degree polynomials over. *Journal of Physics A: Mathematical and Theoretical*, 50(8):084002, 2017.

[33] Atsushi Matsuo and Shigeru Yamashita. Changing the gate order for optimal lnn conversion. In *International Workshop on Reversible Computation*, pages 89–101. Springer, 2011.

[34] Beatrice Nash, Vlad Gheorghiu, and Michele Mosca. Quantum circuit optimizations for nisq architectures. *Quantum Science and Technology*, 5(2):025010, 2020.

[35] Ryan O’Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[36] Alexandru Paler. On the influence of initial qubit placement during nisq circuit compilation. In *International Workshop on Quantum Technology and Optimization Problems*, pages 207–217. Springer, 2019.

[37] Ketan N Patel, Igor L Markov, and John P Hayes. Optimal synthesis of linear reversible circuits. *Quantum Information & Computation*, 8(3):282–294, 2008.

[38] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[39] Massoud Pedram and Alireza Shafaei. Layout optimization for quantum circuits with linear nearest neighbor architectures. *IEEE Circuits and Systems Magazine*, 16(2):62–74, 2016.

[40] Alexandru Paler, Alwin Zulehner, and Robert Wille. Nisq circuit compilation is the travelling salesman problem on a torus. *Quantum Science and Technology*, 2021.

[41] Daniel Ruffinelli and Benjamín Barán. Linear nearest neighbor optimization in quantum circuits: a multiobjective perspective. *Quantum Information Processing*, 16(9):220, 2017.

[42] Md Mazder Rahman and Gerhard W Dueck. Synthesis of linear nearest neighbor quantum circuits. *arXiv preprint arXiv:1508.05430*, 2015.

[43] Matthew Reagor, Christopher B Osborn, Nikolas Tezak, Alexa Staley, Guenevere Prawiroatmodjo, Michael Scheer, Nasser Alidoust, Eyob A Sete, Nicolas Didier, Marcus P da Silva, et al. Demonstration of universal parametric entangling gates on a multi-qubit lattice. *Science advances*, 4(2):eaao3603, 2018.

[44] Victor J Rayward-Smith and A Clare. On finding steiner vertices. *Networks*, 16(3):283–294, 1986.

[45] Gabriel Robins and Alexander Zelikovsky. Tighter bounds for graph steiner tree approximation. *SIAM Journal on Discrete Mathematics*, 19(1):122–134, 2005.

[46] Afshin Sadeghi and Holger Fröhlich. Steiner tree methods for optimal sub-network identification: an empirical study. *BMC bioinformatics*, 14(1):144, 2013.

[47] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[48] Vivek V Shende and Igor L Markov. On the cnot-cost of toffoli gates. *Quantum Information & Computation*, 9(5):461–486, 2009.

[49] Vivek V Shende, Aditya K Prasad, Igor L Markov, and John P Hayes. Reversible logic circuit synthesis. In *Proceedings of the 2002 IEEE/ACM international conference on Computer-aided design*, pages 353–360, 2002.

[50] Marcos Yukio Siraichi, Vinícius Fernandes dos Santos, Sylvain Collange, and Fernando Magno Quintão Pereira. Qubit allocation. In *Proceedings of the 2018 International Symposium on Code Generation and Optimization*, pages 113–125, 2018.

[51] Alireza Shafaei, Mehdi Saeedi, and Massoud Pedram. Optimization of quantum circuits for interaction distance in linear nearest neighbor architectures. In *2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2013.

[52] Alireza Shafaei, Mehdi Saeedi, and Massoud Pedram. Qubit placement to minimize communication overhead in 2d quantum architectures. In *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 495–500. IEEE, 2014.

[53] Mehdi Saeedi, Robert Wille, and Rolf Drechsler. Synthesis of quantum circuits for linear nearest neighbor architectures. *Quantum Information Processing*, 10(3):355–377, 2011.

[54] Yao Tang. Efficient cnot synthesis for nisq devices. *arXiv preprint arXiv:2011.06760*, 2020.

[55] Davide Venturelli, Minh Do, Eleanor Rieffel, and Jeremy Frank. Compiling quantum circuits to realistic hardware architectures using temporal planners. *Quantum Science and Technology*, 3(2):025004, 2018.

[56] Richard Versluis, Stefano Poletto, Nader Khammassi, Brian Tarasinski, Nadia Haider, David J Michalak, Alessandro Bruno, Koen Bertels, and Leonardo DiCarlo. Scalable quantum circuit and control for a superconducting surface code. *Physical Review Applied*, 8(3):034021, 2017.

[57] SM Wang. A multiple source algorithm for suboptimum steiner trees in graphs. In *Proc. International Workshop on Graphtheoretic Concepts in Computer Science (H. Noltemeier, ed.), Traun, W urzburg*, pages 387–396, 1985.

[58] Robert Wille, Lukas Burgholzer, and Alwin Zulehner. Mapping quantum circuits to ibm qx architectures using the minimal number of swap and h operations. In *2019 56th ACM/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2019.

[59] Jonathan Welch, Daniel Greenbaum, Sarah Mostame, and Alán Aspuru-Guzik. Efficient quantum circuits for diagonal unitaries without ancillas. *New Journal of Physics*, 16(3):033040, 2014.

[60] Bujiao Wu, Xiaoyu He, Shuai Yang, Lifu Shou, Guojing Tian, Jialin Zhang, and Xiaoming Sun. Optimization of cnot circuits on topological superconducting processors. *arXiv preprint arXiv:1910.14478*, 2019.

[61] Robert Wille, Oliver Keszocze, Marcel Walter, Patrick Rohrs, Anupam Chattopadhyay, and Rolf Drechsler. Look-ahead schemes for nearest neighbor optimization of 1d and 2d quantum

circuits. In *2016 21st Asia and South Pacific design automation conference (ASP-DAC)*, pages 292–297. IEEE, 2016.

[62] Alwin Zulehner, Alexandru Paler, and Robert Wille. An efficient methodology for mapping quantum circuits to the ibm qx architectures. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 38(7):1226–1236, 2018.

## A Steiner tree algorithm

In this section we describe a heuristic approximation algorithm to find a minimal Steiner tree [46]. It starts by considering each terminal as a separate graph (step 1). Then sequentially we merge the subgraphs that are closest to each other (step 3-7). The distance between two graphs  $f_i$  and  $f_j$  is measured by the shortest distance between any pair of nodes  $u_i, u_j$  such that  $u_i \in f_i$  and  $u_j \in f_j$  (step 4). If we have a sub-graph  $f_i$  having all the terminal nodes then we construct a minimum spanning tree (9)  $T$  on  $f_i$  and remove all non-terminal nodes of degree 1 [10]. The resultant tree is returned as a minimum Steiner tree.

---

**Algorithm 7:** Steiner Tree Algorithm

---

**Input:** (i) A graph  $G = (V, E)$ , (ii) Terminal set  $\mathcal{S} = \{s_1, \dots, s_k\} \subseteq V$   
**Output:** A Steiner tree constructed from  $G$

- 1 Construct a forest  $F$  of  $k$  sub-graphs  $f_1, \dots, f_k$  consisting of one terminal each ;
- 2 **while** does not exist a  $f_i \in F$  such that all terminals  $s_1, \dots, s_k \in f_i$  **do**
- 3     **for** all  $i \neq j$  **do**
- 4         | Determine the shortest path between all nodes in  $f_i$  to all those in  $f_j$  ;
- 5     **end**
- 6     Find the minimum length path  $P$  among all computed paths ;
- 7     Construct  $f_n = f_i \cap f_j \cap P$  and add it to forest  $F$  ;
- 8 **end**
- 9 Construct a minimum spanning tree  $T$  on  $f_i$  ;
- 10 Remove non-terminal nodes of degree 1 from  $T$  ;
- 11 **return**  $T$  ;

---

## B An example for LINEAR-TF-SYNTH

In this section we illustrate Algorithm 1 (LINEAR-TF-SYNTH) with an example taken from [34]. Suppose we have the linear transformation matrix  $A$  and connectivity graph  $G$ , as shown in Figure 3. For simplicity, we have removed the column  $\mathbf{b}$  ( $7^{th}$  column of  $A$ ), since it is all 0 and hence implies there are no X gates to be placed. So this column does not affect any step of the following computations, which are done for the placement of the CNOT gates.

### B.1 Reducing to upper triangular form

We now illustrate the steps to reduce  $A$  to upper triangular form and the way the CNOTs are placed respecting the connectivity constraints. For each column  $i$ , the pivot row is the  $i^{th}$  one. By

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

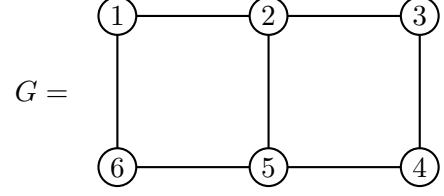
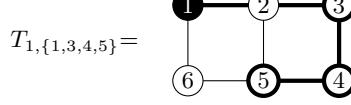


Figure 3: The linear transformation matrix  $A$  and connectivity graph  $G$ .

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$



$$T_1 = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$$

$$T_2 = \begin{bmatrix} 3 & 4 \end{bmatrix}$$

$$T_3 = \begin{bmatrix} 4 & 5 \end{bmatrix}$$

Figure 4: The Steiner tree  $T_{1,S}$  with pivot at 1 and terminals  $S = \{1, 3, 4, 5\}$ .  $T_1, T_2$  and  $T_3$  are the sub-trees built from it.

“fixing” a column  $i$  we mean applying a number of row operations such that  $A_{ii} = 1$  and  $A_{ji} = 0$  for every  $j > i$ . We start fixing from the first column. To save redundancies in explanations, we will make the descriptions from the second column less explicit.

## Column 1

In this column  $A_{11} = A_{31} = A_{41} = A_{51} = 1$ . So we draw a Steiner tree  $T_{1,S}$  with terminals  $S = \{1, 3, 4, 5\}$  and root/pivot at 1 (Figure 4). We call this “pivot”, to distinguish from the roots of each sub-tree that will be built from this tree. The sub-trees  $T_1, T_2$  and  $T_3$  are built by traversing  $T_{1,S}$  breadth-first (Algorithm 3:SEPARATE). As soon as we reach a terminal we stop and build the next sub-tree with that terminal as the root. Thus in each sub-tree, the root and leaves are terminals and remaining nodes are Steiner nodes.

To place the CNOTs we start from the last sub-tree  $T_3$  and use Algorithm 2 (ROW-OP). We have to perform Top-Down-1 first and place CNOT<sub>45</sub>. The 4<sup>th</sup> row of  $A$  gets XORed with the 5<sup>th</sup> row of  $A$ . If we denote the  $j^{\text{th}}$  row of  $A$  by  $A[j, .]$  then  $A[5, .] \leftarrow A[5, .] \oplus A[4, .]$ , remaining rows are unchanged. There are no operations for Bottom-Up-2 in case of  $T_3$ , since there are no Steiner nodes. By similar reasoning we traverse by Top-Down-1 in  $T_2$  and place CNOT<sub>34</sub>, while  $A[4, .] \leftarrow A[4, .] \oplus A[3, .]$ . There are no operations for Bottom-Up-2 in case of  $T_2$  as well. We apply Top-Down-1 in  $T_1$  and get the sequence of operations CNOT<sub>12</sub>, CNOT<sub>23</sub> and the corresponding sequence of matrix operations  $A[2, .] \leftarrow A[2, .] \oplus A[1, .]$  and  $A[3, .] \leftarrow A[3, .] \oplus A[2, .]$ . Then we apply Bottom-Up-2 and place CNOT<sub>12</sub>. The corresponding matrix operations are  $A[2, .] \leftarrow A[2, .] \oplus A[1, .]$ .

Thus the sequence of CNOT operations obtained and the corresponding row operations can be summarized as follows:

$$\begin{aligned} \mathcal{Y}_1^1 &= \{\text{CNOT}_{45}, \text{CNOT}_{34}, \text{CNOT}_{12}, \text{CNOT}_{23}, \text{CNOT}_{12}\} \\ \mathcal{A}_1^1 &= \{A[5, .] \leftarrow A[5, .] \oplus A[4, .], A[4, .] \leftarrow A[4, .] \oplus A[3, .], A[2, .] \leftarrow A[2, .] \oplus A[1, .], \\ &\quad A[3, .] \leftarrow A[3, .] \oplus A[2, .], A[2, .] \leftarrow A[2, .] \oplus A[1, .]\} \end{aligned}$$

$$A = \begin{bmatrix} 1 & \mathbf{1} & 0 & 1 & 1 & 0 \\ 0 & \mathbf{0} & 1 & 1 & 0 & 1 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 1 & 1 & 0 \\ 0 & \mathbf{0} & 1 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 1 & 0 & 1 \end{bmatrix}$$

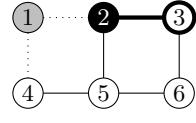


Figure 5: Since  $A_{22} = 0$  so we apply  $\text{CNOT}_{32}$  and “propagate” 1 from  $A_{32}$  to  $A_{22}$ .

$$A = \begin{bmatrix} 1 & \mathbf{1} & 0 & 1 & 1 & 0 \\ 0 & \mathbf{1} & 1 & 1 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 1 & 1 & 0 \\ 0 & \mathbf{0} & 1 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 1 & 0 & 1 \end{bmatrix}$$

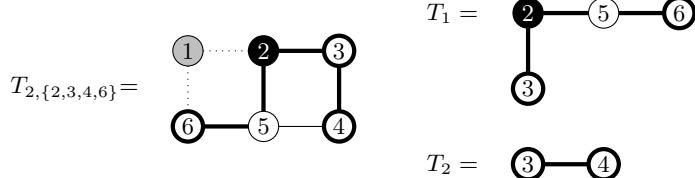


Figure 6: The Steiner tree  $T_{2,S}$  with pivot at 2 and terminals  $S = \{2, 3, 4, 6\}$ .  $T_1$  and  $T_2$  are the sub-trees built from it.

$$\text{The matrix } A \text{ after all these operations is as follows : } A = \begin{bmatrix} 1 & \mathbf{1} & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 1 & 0 & 1 \end{bmatrix}$$

## Column 2

Now we fix column 2. Since  $A_{22} = 0$  after fixing the first column (first image in Figure 5) so we try to propagate 1 from a row below it. In this case the nearest node to 2 in the graph, that has a 1 in the matrix, is 3. So we apply  $\text{CNOT}_{32}$  and the corresponding row operation is as follows:

$$\begin{aligned} \mathcal{Y}_1^{2'} &= \{\text{CNOT}_{32}\} \\ \mathcal{A}_1^{2'} &= \{A[2, :] \leftarrow A[2, :] \oplus A[3, :]\} \end{aligned}$$

The matrix  $A$  after this operation is as shown in the beginning of Figure 6. Now the pivot is at 2 and the set of terminal nodes is  $S = \{2, 3, 4, 6\}$ . We draw the Steiner tree  $T_{2,S}$  in the graph  $G \setminus \{1\}$  and divide it into sub-trees as shown in Figure 6, using the same procedure as described before. Then we traverse the sub-trees using ROW-OP (Algorithm 2) and get the following sequence of CNOTs and the corresponding row operations for  $A$ .

$$\begin{aligned} \mathcal{Y}_1^2 &= \{\text{CNOT}_{34}, \text{CNOT}_{23}, \text{CNOT}_{25}, \text{CNOT}_{56}, \text{CNOT}_{25}\} \\ \mathcal{A}_1^2 &= \{A[4, :] \leftarrow A[4, :] \oplus A[3, :], A[3, :] \leftarrow A[3, :] \oplus A[2, :], \\ &\quad A[5, :] \leftarrow A[5, :] \oplus A[2, :], A[6, :] \leftarrow A[6, :] \oplus A[5, :], A[5, :] \leftarrow A[5, :] \oplus A[2, :]\} \end{aligned}$$

## Column 3

The state of  $A$  before fixing column 3 i.e. after applying all the previous operations is as shown in the beginning of Figure 7. We draw the Steiner tree  $T_{3,S}$  in the graph  $G \setminus \{1, 2\}$  using the set

$$A = \begin{bmatrix} 1 & 1 & \mathbf{0} & 1 & 1 & 0 \\ 0 & 1 & \mathbf{1} & 1 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{0} & 0 & 0 & 1 \end{bmatrix}$$

$$T_{3,\{3,4,5\}} =$$

$$T_1 =$$

$$T_2 =$$

Figure 7: The Steiner tree  $T_{3,\mathcal{S}}$  with pivot at 3 and terminals  $\mathcal{S} = \{3, 4, 5\}$ .  $T_1$  and  $T_2$  are the sub-trees built from it.

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 1 & \mathbf{1} & 0 & 1 \\ 0 & 0 & 0 & \mathbf{0} & 1 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 0 & \mathbf{0} & 0 & 1 \end{bmatrix}$$

Figure 8: Since  $A_{44} = 0$  so we apply  $\text{CNOT}_{54}$  and “propagate” 1 from  $A_{54}$  to  $A_{44}$ .

of terminals  $\mathcal{S} = \{3, 4, 5\}$ . Then we sub-divide into sub-trees and get the following sequence of CNOTS and row operations, after traversing them according to ROW-OP (Algorithm 2).

$$\mathcal{Y}_1^3 = \{\text{CNOT}_{45}, \text{CNOT}_{34}\}$$

$$\mathcal{A}_1^3 = \{A[5, .] \leftarrow A[5, .] \oplus A[4, .], A[4, .] \leftarrow A[4, .] \oplus A[3, .]\}$$

#### Column 4

The matrix obtained after applying the previous operations is shown in Figure 8. Since  $A_{44} = 0$  we have to propagate a 1 from a row below it. In this case node 5 is the nearest to node 4 and has a 1. So we apply the following CNOT and the corresponding row operation.

$$\mathcal{Y}_1^4 = \{\text{CNOT}_{54}\}$$

$$\mathcal{A}_1^4 = \{A[4, .] \leftarrow A[4, .] \oplus A[5, .]\}$$

After this we extract a Steiner tree  $T_{4,\mathcal{S}}$  from  $G \setminus \{1, 2, 3\}$  with pivot 4 and set of terminals as  $\mathcal{S} = \{4, 5\}$ . Traversing this tree (no sub-trees here) we get the following operations.

$$\mathcal{Y}_1^4 = \{\text{CNOT}_{45}\}$$

$$\mathcal{A}_1^4 = \{A[5, .] \leftarrow A[5, .] \oplus A[4, .]\}$$

After these operations we find that column 5 and 6 are fixed. So  $A$  has been reduced to an upper triangular form.

#### B.2 Transpose and reducing to identity

Now we transpose  $A$ , as shown in Figure 10 and fix each column such that 1 remains only in the diagonal.

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad T_{4,\{4,5\}} = \begin{array}{c} (1) \cdots (2) \cdots (3) \\ \vdots \quad \vdots \quad \vdots \\ (6) - (5) - (4) \end{array} \quad T_1 = \begin{array}{c} (4) - (5) \end{array}$$

Figure 9: The Steiner tree  $T_{4,\mathcal{S}}$  with pivot at 4 and terminals  $\mathcal{S} = \{4, 5\}$ .

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad T_{1,\{1,2,4,5\}} = \begin{array}{c} (1) - (2) - (3) \\ | \quad | \quad | \\ (6) - (5) - (4) \end{array} \quad T_1 = \begin{array}{c} (1) - (2) \end{array} \\ T_2 = \begin{array}{c} (2) - (5) \end{array} \\ T_3 = \begin{array}{c} (5) - (4) \end{array}$$

Figure 10: The Steiner tree  $T_{1,\mathcal{S}}$  with pivot at 1 and terminals  $\mathcal{S} = \{1, 2, 4, 5\}$ .  $T_1, T_2$  and  $T_3$  are the sub-trees built from it.

## Column 1

We build a Steiner tree  $T_{1,\{\mathcal{S}\}}$  (Figure 10) with pivot 1 and set of terminals  $\mathcal{S} = \{1, 2, 4, 5\}$ . We divide into sub-trees according to Algorithm 3 (SEPARATE) and do the traversals in each sub-tree, starting from the last one built, according to ROW-OP (Algorithm 2). This time we apply Bottom-Up-1, Top-Down-1, Bottom-Up-2 and Top-Down-2 and get the following sequence of CNOTs and row operations on  $A$ .

$$\begin{aligned} \mathcal{Y}_2^1 &= \{\text{CNOT}_{54}, \text{CNOT}_{25}, \text{CNOT}_{12}\} \\ \mathcal{A}_2^1 &= \{A[4, .] \leftarrow A[4, .] \oplus A[5, .], A[5, .] \leftarrow A[5, .] \oplus A[2, .], A[2, .] \leftarrow A[2, .] \oplus A[1, .]\} \end{aligned}$$

The purpose of applying all the sub-procedures is as follows. Let the parity at root and leaf before traversal is  $x_r$  and  $x_\ell$  respectively. After applying Bottom-Up-1, Top-Down-1, Bottom-Up-2, Top-Down-2 the parity at leaf is  $x'_\ell = x_r \oplus x_\ell$ . The parities at the other nodes remain unchanged.

Thus after Bottom-Up-1+Top-Down-1+Bottom-Up-2+Top-Down-2 on sub-tree  $T_3$ , which in this case is a single CNOT<sub>54</sub>, the parity at node 4 is  $x'_4 = x_4 \oplus x_5$ , and parity at 5 is unchanged. Similarly after applying the traversals in  $T_2$ , the parity at 5 is  $x'_5 = x_5 \oplus x_2$  and the parity at 2 is unchanged. After traversing  $T_1$  the parity at 2 is  $x'_2 = x_2 \oplus x_1$  and the parity at 1 is unchanged.

Now to avoid disturbing the upper-triangular 0s, we want that a node (row) should be XORed with a row with a higher index, which is clearly violated in case of  $T_3$  where we have  $x_4 \oplus x_5$  at node 4. So we apply a correction procedure, by Algorithm 1 (LINEAR-TF-SYNTH), after traversing all sub-trees. We take the shortest path from 5 to 4, which in this case is  $T_3$ , and again apply the same traversals. Thus we get the following sequence of CNOTs.

$$\begin{aligned} \mathcal{Y}_2^{1'} &= \{\text{CNOT}_{54}\} \\ \mathcal{A}_2^{1'} &= \{A[4, .] \leftarrow A[4, .] \oplus A[5, .]\} \end{aligned}$$

Then the parity at 4 becomes  $x'_4 \oplus x'_5 = (x_4 \oplus x_5) \oplus (x_5 \oplus x_2) = x_4 \oplus x_2$ , which satisfies the desired condition.

$$A = \begin{bmatrix} 1 & \mathbf{0} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 1 & 0 & 0 & 0 \\ 0 & \mathbf{0} & 1 & 1 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 1 & 0 \\ 0 & \mathbf{0} & 1 & 1 & 0 & 1 \end{bmatrix}$$

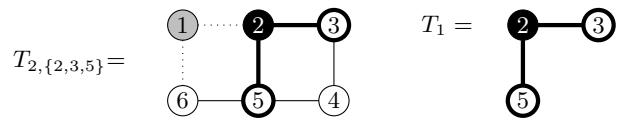


Figure 11: The Steiner tree  $T_{2,S}$  with pivot at 2 and terminals  $S = \{2, 3, 5\}$ .

$$A = \begin{bmatrix} 1 & 1 & \mathbf{0} & 0 & 0 & 0 \\ 0 & 1 & \mathbf{0} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} & 0 & 1 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 & 1 \end{bmatrix}$$

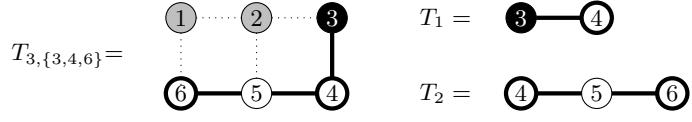


Figure 12: The Steiner tree  $T_{3,S}$  with pivot at 3 and terminals  $S = \{3, 4, 6\}$ .  $T_1$  and  $T_2$  are the sub-trees built from it.

## Column 2

The state of the matrix  $A$  after applying the previous operations is shown in Figure 11. To fix column 2, we draw a Steiner tree  $T_{2,S}$  on the graph  $G \setminus \{1\}$ , with pivot 2 and set of terminals  $S = \{2, 3, 5\}$ . We invoke procedure ROW-OP (Algorithm 2) and get the following sequence of CNOTs and row operations.

$$\begin{aligned} \mathcal{Y}_2^2 &= \{\text{CNOT}_{23}, \text{CNOT}_{25}\} \\ \mathcal{A}_2^2 &= \{A[3, .] \leftarrow A[3, .] \oplus A[2, .], A[5, .] \leftarrow A[5, .] \oplus A[2, .]\} \end{aligned}$$

This time all the rows are XORed with a row with a higher index. So no correction procedures are required.

## Column 3

The state of  $A$  after the previous operations is shown in Figure 12. As before we build a Steiner tree  $T_{3,S}$  on  $G \setminus \{1, 2\}$  with pivot 3 and set of terminals  $S = \{3, 4, 6\}$ , which is further sub-divided into sub-trees  $T_1$  and  $T_2$ . Applying the traversals according to ROW-OP (Algorithm 2) we get the following sequence of CNOTs and corresponding row operations.

$$\begin{aligned} \mathcal{Y}_2^3 &= \{\text{CNOT}_{56}, \text{CNOT}_{45}, \text{CNOT}_{56}, \text{CNOT}_{45}, \text{CNOT}_{34}\} \\ \mathcal{A}_2^3 &= \{A[6, .] \leftarrow A[6, .] \oplus A[5, .], A[5, .] \leftarrow A[5, .] \oplus A[4, .], \\ &\quad A[6, .] \leftarrow A[6, .] \oplus A[5, .], A[5, .] \leftarrow A[5, .] \oplus A[4, .], A[4, .] \leftarrow A[4, .] \oplus A[3, .]\} \end{aligned}$$

After all these operations we get  $A = \mathbb{I}$ .

### B.3 The complete circuit synthesizing a linear transformation matrix

Let  $\mathcal{Y}_1$  be the sequence (in order) of CNOTs obtained while reducing to upper triangular form.  $\mathcal{Y}_2$  is the sequence of CNOTs obtained after transpose and before reducing to identity.  $\mathcal{Y}_2'$  is the

same sequence of CNOTs as in  $\mathcal{Y}_2$ , but with the control and target flipped. Then the final circuit is  $\mathcal{Y} = \mathcal{Y}'_2 \circ \text{reverse}(\mathcal{Y}_1)$ , where  $\circ$  means that we concatenate the reverse sequence in  $\mathcal{Y}_1$  after  $\mathcal{Y}'_2$ .

The number of CNOTs used by our algorithm is 26, while the algorithm in [34] used 43 CNOTs. So our algorithm fares much better in terms of CNOT requirement.

## C An example for PHASE-NW-SYNTH

In this we illustrate Algorithm 4 (PHASE-NW-SYNTH) with the connectivity graph  $G$  given in Figure 3. The input consists of the following parity terms and their coefficients. The number of qubits  $n = 6$ .

$$\mathcal{P} = \{(1, 1 \oplus x_1 \oplus x_4 \oplus x_5), (2, x_2 \oplus x_3 \oplus x_5 \oplus x_6), (4, 1 \oplus x_4 \oplus x_5 \oplus x_6), (4, 1 \oplus x_1 \oplus x_2 \oplus x_6), (6, 1 \oplus x_1 \oplus x_2 \oplus x_3), (7, 1 \oplus x_1 \oplus x_2 \oplus x_4 \oplus x_6), (1, x_2 \oplus x_4 \oplus x_5)\} \quad (7)$$

$$P = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 4 & 4 & 6 & 7 & 1 \end{bmatrix}$$

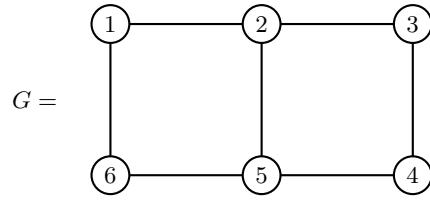


Figure 13: The parity matrix  $P_{8 \times 7}$  and connectivity graph  $G$ .

The parity matrix  $P$  is a  $8 \times 7$  matrix where each column represents a parity term in  $\mathcal{P}$ . The first 6 rows in each column encode the parity (without bit flip), the 7<sup>th</sup> row encodes the bit flip term and the last row stores the coefficients. The matrix  $P$  and the connectivity graph  $G$  has been shown in Figure 13. We represent the set  $B$  as a matrix where each column is a parity term ( $p$ ) without the bit flip variable. We label column  $i$  by “ $p_i$ ”. In this section superscripts denote the iteration we are in.

$$B^{(0)} = \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

We initialize an empty stack  $\mathcal{K}$ ,  $I = [6]$ . We describe each iteration of the algorithm. A stack is a first-in and last-out data structure. From here on, we represent the stack  $\mathcal{K}$  as an ordered set, where the rightmost element is the last one in or the element at the top of the stack. The leftmost element is the one at the bottom of the stack.

### Iteration 1

We select  $j = 2$  as the pivot row, according to step 25 in Algorithm 4. The 0-cofactor ( $B_0^1$ ) and 1-cofactor ( $B_1^1$ ) are the columns which has 0 and 1 in the  $j^{\text{th}}$  row respectively. The stack  $\mathcal{K}$  is as

follows.

$$\begin{aligned} B_1^1 &= \{p_2, p_4, p_5, p_6, p_7\} \quad \text{and} \quad B_0^1 = \{p_1, p_3\} \\ \mathcal{K} &= \{(B_1^1, I \setminus \{2\}, 2), (B_0^1, I \setminus \{2\}, \epsilon)\} \end{aligned}$$

The stack contains tuples  $(B', I, i)$ , in which the first element is a subset of columns of  $B$ . The second element  $I \subseteq [6]$  indicates which rows in  $B'$  have not been considered as ‘‘pivot’’. We divide a set of columns into 0 and 1-cofactor, depending upon the entries in the pivot row. The third element  $i$  is the index of the pivot row, according to which the columns in  $B'$  became part of a 1-cofactor for the first time.

At the beginning, if no such pivot row is encountered for a set of columns (for example, in 0-cofactors) then we initialize the third element to some  $\epsilon \notin [6]$ . Once third element has some value in  $[6]$ , it remains unchanged for the columns in  $B'$  throughout the algorithm, even if  $B'$  is further sub-divided.

## Iteration 2

We pop  $(B_0^1, I \setminus \{2\}, \epsilon)$  from the top of the stack  $\mathcal{K}$ . We select  $j = 1$  as the pivot row. The 0-cofactor, 1-cofactor and  $\mathcal{K}$  are as follows.

$$\begin{aligned} B_1^2 &= \{p_1\} \quad \text{and} \quad B_0^2 = \{p_3\} \\ \mathcal{K} &= \{(B_1^1, I \setminus \{2\}, 2), (B_1^2, I \setminus \{2, 1\}, 1), (B_0^2, I \setminus \{2, 1\}, \epsilon)\} \end{aligned}$$

## Iteration 3

We pop  $(B_0^2, I \setminus \{2, 1\}, \epsilon)$  from the top of  $\mathcal{K}$  and select  $j = 4$  as the pivot row. The 0-cofactor, 1-cofactor and  $\mathcal{K}$  is as follows.

$$\begin{aligned} B_1^3 &= \{p_3\} \quad \text{and} \quad B_0^3 = \emptyset \\ \mathcal{K} &= \{(B_1^1, I \setminus \{2\}, 2), (B_1^2, I \setminus \{2, 1\}, 1), (B_1^3, I \setminus \{2, 1, 4\}, 4)\} \end{aligned}$$

## Iteration 4

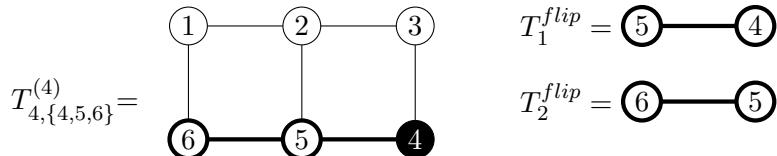
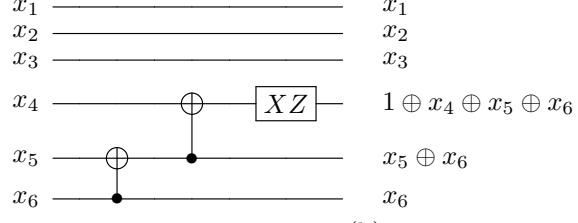


Figure 14: The Steiner tree  $T_{4,\{4,5,6\}}^{(4)}$  (iteration 4). The sub-trees  $T_1$  and  $T_2$  are are flipped such that root becomes leaf and vice-versa.

We pop  $(B_1^3, I \setminus \{2, 1, 4\}, 4)$  from the top of  $\mathcal{K}$ . Since the third element of the tuple is an integer, so we go to step 11 in Algorithm 4 and check if there is a set  $\mathcal{S}'$  of rows such that all columns in  $B_1^3 = \{p_3\}$  have a 1. We find  $\mathcal{S}' = \{5, 6\}$ . We then build a Steiner tree  $T_{4,\mathcal{S}}^{(4)}$  on  $G$  with set  $\mathcal{S} = \{4, 5, 6\}$  of terminals and ‘‘pivot node’’ as 4 (Figure 14). Then we divide the tree into sub-trees as described in Algorithm 3 (SEPARATE). If a sub-tree has multiple leaves we make each path as

$$B^{(4)} = \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

(a)



(b)

Figure 15: (a)  $B$  after applying row operations in iteration 4. (b) The partial circuit obtained after applying the sequence of gates obtained from iteration 4. The variables on the left and right denote the parities before and after the application of the gates respectively.

a separate sub-tree. We flip the root and leaf of each sub-tree and invoke Algorithm 2 (ROW-OP) where we get the sequence of CNOTs according to the 4 traversals : Bottom-Up-1, Top-Down-1, Bottom-Up-2, Top-Down-2. The row operations invoked on  $B$  depend only on the root and leaf of each sub-tree.

$$\begin{aligned} \mathcal{V} &= \{\text{CNOT}_{65}, \text{CNOT}_{54}\} \\ \mathcal{A} &= \{B[6, .] \leftarrow B[6, .] \oplus B[5, .], B[5, .] \leftarrow B[5, .] \oplus B[4, .]\} \end{aligned}$$

$B$  after the row operations and the partial circuit has been shown in Figure 15. We find that column  $p_3$  has been fixed i.e. there is a single 1 and rest are 0. This implies that the 3<sup>rd</sup> parity in  $P$  is realized. Since  $P_{73} = 1$ , so the bit-flip variable is set to 1. The coefficient  $P_{83} = 4$ . So we need to place X and Z gate at the point in the circuit where the parity has been realized. The stack  $\mathcal{K} = \{(B_1^1, I \setminus \{2\}, 2), (B_1^2, I \setminus \{2, 1\}, 1)\}$ . Also, after this point we remove the column  $p_3$  from  $B$ .

## Iteration 5

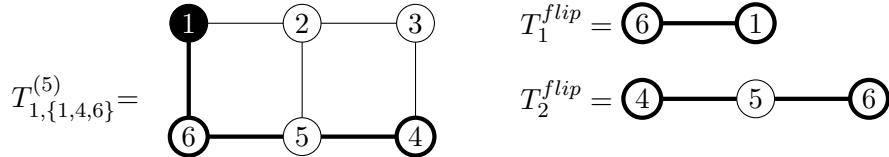


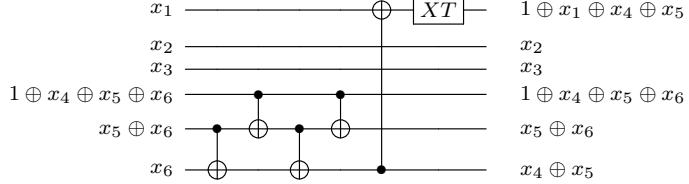
Figure 16: The Steiner tree  $T_{1,\{1,4,6\}}^{(5)}$  (iteration 5). Sub-trees  $T_1$  and  $T_2$  are flipped such that root becomes leaf and vice-versa.

We pop  $(B_1^2, I \setminus \{2, 1\}, 1)$  from  $\mathcal{K}$  where  $B_1^2 = \{p_1\}$ . As explained in the previous iteration we go to step 11 in Algorithm 4 and find  $\mathcal{S}' = \{4, 6\}$ . Thus we build a Steiner tree  $T_{1,\mathcal{S}}^{(5)}$  on  $G$  with set of terminals  $\mathcal{S} = \{1, 4, 6\}$  and pivot node at 1 (Figure 16). Then we separate into two sub-trees and flip them, obtaining  $T_1^{flip}$  and  $T_2^{flip}$ . After applying the traversals in Algorithm 2 (ROW-OP) we get the following sequence of CNOTs and row operations.

$$\begin{aligned} \mathcal{V} &= \{\text{CNOT}_{56}, \text{CNOT}_{45}, \text{CNOT}_{56}, \text{CNOT}_{45}, \text{CNOT}_{61}\} \\ \mathcal{A} &= \{B[4, .] \leftarrow B[4, .] \oplus B[6, .], B[6, .] \leftarrow B[6, .] \oplus B[1, .]\} \end{aligned}$$

$$B^{(5)} = \begin{bmatrix} p_1 & p_2 & p_4 & p_5 & p_6 & p_7 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

(a)



(b)

Figure 17: (a)  $B$  after applying row operations in iteration 5. (b) The partial circuit obtained after applying the sequence of gates obtained from iteration 5. The variables on the left and right denote the parities before and after the application of the gates respectively.

Applying these operations we find that  $p_1$  has been fixed (Figure 17). So we remove this column, append the sequence of CNOTs and according to the bit flip variable value ( $P_{71} = 1$ ) and coefficient ( $P_{81} = 1$ ) we place X and T gate at the place where the 1<sup>st</sup> parity in  $P$  has been realized. Now stack has  $\mathcal{K} = \{(B_1^1, I \setminus \{2, \}, 2)\}$ .

### Iteration 6

We pop  $(B_1^1, I \setminus \{2, \}, 2)$  from the top of  $\mathcal{K}$ , where  $B_1^1 = \{p_2, p_4, p_5, p_6, p_7\}$ . We select  $j = 1$  as the pivot row according to step 25 of Algorithm 4. Now the 0-cofactor, 1-cofactor and stack are as follows.

$$\begin{aligned} B_1^6 &= \{p_4, p_5, p_6\} \quad \text{and} \quad B_0^6 = \{p_2, p_7\} \\ \mathcal{K} &= \{(B_1^6, I \setminus \{2, 1\}, 2), (B_0^6, I \setminus \{2, 1\}, 2)\} \end{aligned}$$

### Iteration 7

We pop  $(B_0^6, I \setminus \{2, 1\}, 2)$  from the top of  $\mathcal{K}$  and set  $j = 3$  as the pivot row. The 0-cofactor, 1-cofactor and  $\mathcal{K}$  are as follows.

$$\begin{aligned} B_1^7 &= \{p_2\} \quad \text{and} \quad B_0^7 = \{p_7\} \\ \mathcal{K} &= \{(B_1^6, I \setminus \{2, 1\}, 2), (B_1^7, I \setminus \{2, 1, 3\}, 2), (B_0^7, I \setminus \{2, 1, 3\}, 2)\} \end{aligned}$$

### Iteration 8

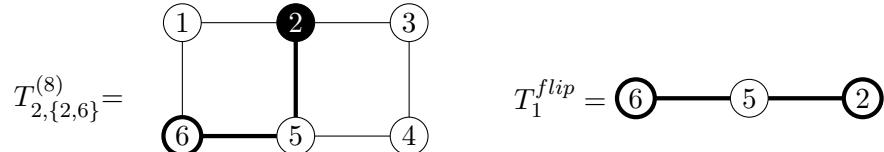
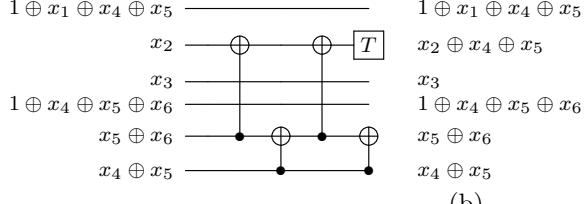


Figure 18: The Steiner tree  $T_{2,\{2,6\}}^{(8)}$  (iteration 8). The single sub-tree is flipped such that root becomes leaf and vice-versa.

We pop  $(B_0^7, I \setminus \{2, 1, 3\}, 2)$  from  $\mathcal{K}$ . According to step 11, we find  $\mathcal{S}' = \{6\}$ . So we build a Steiner tree  $T_{2,\mathcal{S}}^{(8)}$  on  $G$  (Figure 18), with pivot at 2 and set of terminals  $\mathcal{S} = \{2, 6\}$ . Following the

$$B^{(8)} = \begin{bmatrix} \frac{p_2}{0} & \frac{p_4}{1} & \frac{p_5}{1} & \frac{p_6}{1} & \frac{p_7}{0} \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

(a)



(b)

Figure 19: (a)  $B$  after applying row operations in iteration 8. (b) The partial circuit obtained after applying the sequence of gates obtained from iteration 8. The variables on the left and right denote the parities before and after the application of the gates respectively.

traversals in Algorithm 2 (ROW-OP) the sequence of CNOTs and row operations obtained as follows.

$$\begin{aligned} \mathcal{Y} &= \{\text{CNOT}_{52}, \text{CNOT}_{65}, \text{CNOT}_{52}, \text{CNOT}_{65}\} \\ \mathcal{A} &= \{B[6, .] \leftarrow B[6, .] \oplus B[2, .]\} \end{aligned}$$

The state of  $B$  and the partial circuit is shown in Fig 19. According to the value of the bit-flip variable ( $P_{77} = 0$ ) and coefficient ( $P_{87} = 1$ ) we place a T-gate at the place where the 7<sup>th</sup> parity term of  $P$  is realized. The stack is  $\mathcal{K} = \{(B_1^6, I \setminus \{2, 1\}, 2), (B_1^7, I \setminus \{2, 1, 3\}, 2)\}$ . Since  $p_7$  is fixed, so we remove it from  $B$ .

### Iteration 9

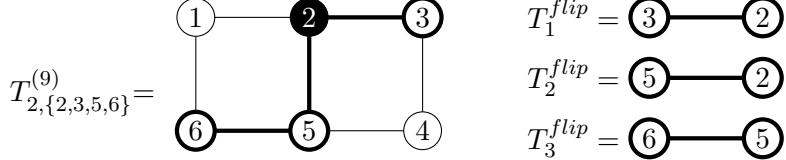


Figure 20: The Steiner tree  $T_{2,\{2,3,5,6\}}^{(9)}$  (iteration 9). The sub-trees are flipped such that root becomes leaf and vice-versa.

We pop  $(B_1^7, I \setminus \{2, 1, 3\}, 2)$  from  $\mathcal{K}$ , where  $B_1^7 = \{p_2\}$ . Similar to iteration 8, we build a Steiner tree  $T_{2,S}$  on  $G$  (Figure 20) with pivot at 2 and set of terminals  $S = \{2, 3, 5, 6\}$ . We get the following sequence of CNOTs and row operations from ROW-OP(Algorithm 2).

$$\begin{aligned} \mathcal{Y} &= \{\text{CNOT}_{65}, \text{CNOT}_{52}, \text{CNOT}_{32}\} \\ \mathcal{A} &= \{B[6, .] \leftarrow B[6, .] \oplus B[5, .], B[5, .] \leftarrow B[5, .] \oplus B[2, .], B[3, .] \leftarrow B[3, .] \oplus B[2, .]\} \end{aligned}$$

The state of  $B$  and the partial circuit has been shown in Figure 21. We remove  $p_2$  from  $B$  since it is fixed. According to the bit flip variable ( $P_{72} = 0$ ) and coefficient ( $P_{82} = 2$ ) in  $P$ , we place S-gate at the place where the parity of column 2 in matrix  $P$  is realized. The stack is  $\mathcal{K} = \{(B_1^6, I \setminus \{2, 1\}, 2)\}$ .

$$\begin{aligned}
B^{(9)} = & \begin{bmatrix} p_2 & p_4 & p_5 & p_6 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} & \begin{array}{l} 1 \oplus x_1 \oplus x_4 \oplus x_5 \\ x_2 \oplus x_4 \oplus x_5 \\ 1 \oplus x_4 \oplus x_5 \oplus x_6 \\ x_5 \oplus x_6 \\ x_4 \oplus x_5 \end{array} & \begin{array}{l} 1 \oplus x_1 \oplus x_4 \oplus x_5 \\ x_2 \oplus x_3 \oplus x_5 \oplus x_6 \\ x_3 \\ 1 \oplus x_4 \oplus x_5 \oplus x_6 \\ x_4 \oplus x_6 \\ x_4 \oplus x_5 \end{array} \\
& \text{(a)} & \text{(b)} & 
\end{aligned}$$

Figure 21: (a)  $B$  after applying row operations in iteration 9. (b) The partial circuit obtained after applying the sequence of gates obtained from iteration 9. The variables on the left and right denote the parities before and after the application of the gates respectively.

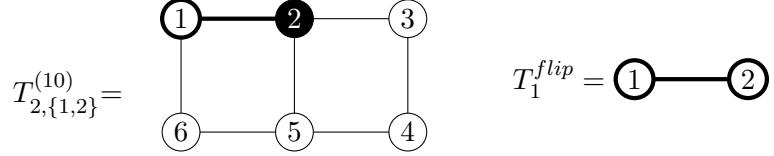


Figure 22: The Steiner tree  $T_{2,\{1,2\}}^{(10)}$  (iteration 10). The single sub-tree is flipped such that root becomes leaf and vice-versa.

## Iteration 10

We now pop  $(B_1^6, I \setminus \{2, 1\}, 2)$ , where  $B_1^6 = \{p_4, p_5, p_6\}$ . At step 11 of Algorithm 4 we find  $\mathcal{S}' = \{1\}$ . Thus we build a Steiner tree  $T_{2,\mathcal{S}}^{(10)}$  (Figure 22) on  $G$  with pivot at 2 and terminal  $\mathcal{S} = \{1, 2\}$ . As before we flip the only sub-tree and obtain the following sequence of gates and row operations.

$$\begin{aligned}
\mathcal{Y} &= \{\text{CNOT}_{12}\} \\
\mathcal{A} &= \{B[1, :] \leftarrow B[1, :] \oplus B[2, :]\}
\end{aligned}$$

No column is fixed (Figure 23), so we go to step 25 and further divide  $B_1^6$  into 0-cofactor and 1-cofactor, by pivoting at  $j = 3$ , and push these into the stack  $\mathcal{K}$ .

$$\begin{aligned}
B_1^{10} &= \{p_4, p_6\} \quad \text{and} \quad B_0^{10} = \{p_5\} \\
\mathcal{K} &= \{(B_1^{10}, I \setminus \{2, 1, 3\}, 2), (B_0^{10}, I \setminus \{2, 1, 3\}, 2)\}
\end{aligned}$$

$$\begin{aligned}
B^{(10)} = & \begin{bmatrix} p_4 & p_5 & p_6 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} & \begin{array}{l} 1 \oplus x_1 \oplus x_4 \oplus x_5 \\ x_2 \oplus x_3 \oplus x_5 \oplus x_6 \\ x_3 \\ 1 \oplus x_4 \oplus x_5 \oplus x_6 \\ x_4 \oplus x_6 \\ x_4 \oplus x_5 \end{array} & \begin{array}{l} 1 \oplus x_1 \oplus x_4 \oplus x_5 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_6 \\ x_3 \\ 1 \oplus x_4 \oplus x_5 \oplus x_6 \\ x_4 \oplus x_6 \\ x_4 \oplus x_5 \end{array} \\
& \text{(a)} & \text{(b)} & 
\end{aligned}$$

Figure 23: (a)  $B$  after applying row operations in iteration 10. (b) The partial circuit obtained after applying the CNOT obtained from iteration 10. The variables on the left and right denote the parities before and after the application of the CNOT respectively.

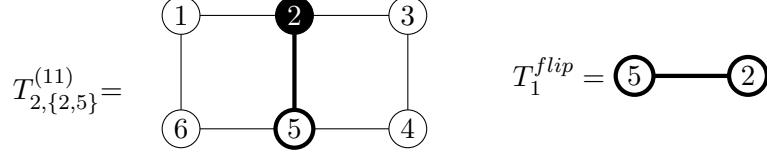


Figure 24: The Steiner tree  $T_{2,\{2,5\}}^{(11)}$  (iteration 11). The single sub-tree is flipped such that root becomes leaf and vice-versa.

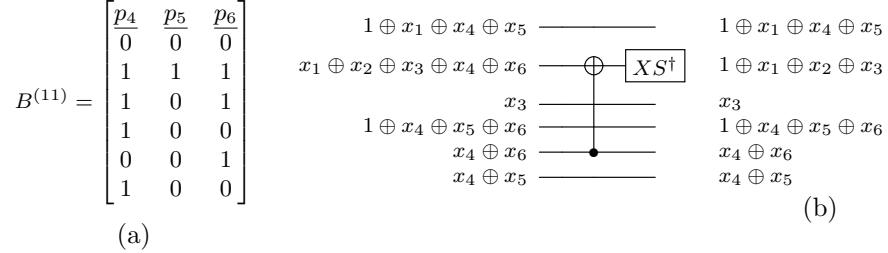


Figure 25: (a)  $B$  after applying row operations in iteration 11. (b) The partial circuit obtained after applying the gates obtained from iteration 11. The variables on the left and right denote the parities before and after the application of the gates respectively.

## Iteration 11

We pop  $(B_0^{10}, I \setminus \{2, 1, 3\}, 2)$  from  $\mathcal{K}$ , where  $B_0^{10} = \{p_5\}$ . From the fifth column we find  $\mathcal{S}' = \{5\}$ . Thus we build a Steiner tree  $T_{2,\mathcal{S}}^{(11)}$  (Figure 24) on  $G$  with pivot at 2 and set of terminals  $\mathcal{S} = \{2, 5\}$ . Flipping and traversing we get the following sequence of CNOTs and row operations.

$$\begin{aligned}\mathcal{Y} &= \{\text{CNOT}_{52}\} \\ \mathcal{A} &= \{B[5, .] \leftarrow B[5, .] \oplus B[2, .]\}\end{aligned}$$

Now the state of  $B$  and the appended circuit is shown in Figure 25, where we see that  $p_5$  has been fixed. Since the value of the bit variable is set ( $P_{75} = 1$ ) and coefficient is  $P_{85} = 6$ , so we place a X and  $S^\dagger$  gate at the place where the 5<sup>th</sup> parity in  $P$  is realized. The stack is  $\mathcal{K} = \{(B_1^{(10)}, I \setminus \{2, 1, 3\}, 2)\}$ .

## Iteration 12

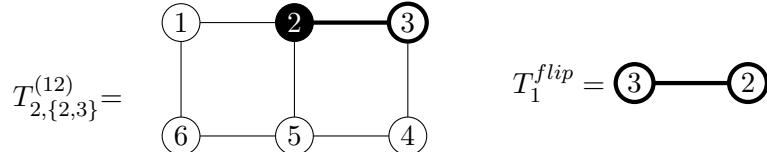


Figure 26: The Steiner tree  $T_{2,\{2,3\}}^{(12)}$  (iteration 12). The single sub-tree is flipped such that root becomes leaf and vice-versa.

We pop  $(B_1^{10}, I \setminus \{2, 1, 3\}, 2)$  from  $\mathcal{K}$ , where  $B_1^{10} = \{p_4, p_6\}$ . At step 11 of Algorithm 4 we find that  $\mathcal{S}' = \{3\}$ . So we build a Steiner tree  $T_{2,\mathcal{S}}$  (Figure 26) on  $G$  with pivot at 2 and set of terminals

$$\begin{aligned}
B^{(12)} &= \begin{bmatrix} p_4 & p_6 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{array}{c} 1 \oplus x_1 \oplus x_4 \oplus x_5 \\ 1 \oplus x_1 \oplus x_2 \oplus x_3 \\ x_3 \\ 1 \oplus x_4 \oplus x_5 \oplus x_6 \\ x_4 \oplus x_6 \\ x_4 \oplus x_5 \end{array} & \begin{array}{c} 1 \oplus x_1 \oplus x_4 \oplus x_5 \\ 1 \oplus x_1 \oplus x_2 \\ x_3 \\ 1 \oplus x_4 \oplus x_5 \oplus x_6 \\ x_4 \oplus x_6 \\ x_4 \oplus x_5 \end{array} \\
(a) & & & (b)
\end{aligned}$$

Figure 27: (a)  $B$  after applying row operations in iteration 12. (b) The partial circuit obtained after applying the gates obtained from iteration 12. The variables on the left and right denote the parities before and after the application of the gates respectively.

as  $\mathcal{S} = \{2, 3\}$ . After flipping and traversing we obtain the following sequence of CNOT gates and row operations.

$$\begin{aligned}
\mathcal{Y} &= \{\text{CNOT}_{32}\} \\
\mathcal{A} &= \{B[3, .] \leftarrow B[3, .] \oplus B[2, .]\}
\end{aligned}$$

The state of  $B$  and the appended circuit has been shown in Figure 27. At step 25 of Algorithm 4 we sub-divide  $B_1^{10}$  by pivoting at  $j = 4$ . We get the following 0-cofactor, 1-cofactor, which we push into the stack.

$$\begin{aligned}
B_1^{12} &= \{p_4\} \quad \text{and} \quad B_0^{12} = \{p_6\} \\
\mathcal{K} &= \{(B_1^{12}, I \setminus \{2, 1, 3, 4\}, 2), (B_0^{12}, I \setminus \{2, 1, 3, 4\}, 2)\}
\end{aligned}$$

### Iteration 13

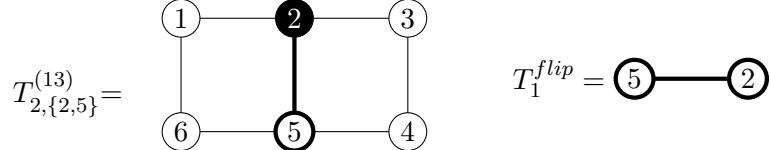


Figure 28: The Steiner tree  $T_{2,\{2,5\}}^{(13)}$  (iteration 13). The single sub-tree is flipped such that root becomes leaf and vice-versa.

We pop  $(B_0^{12}, I \setminus \{2, 1, 3, 4\}, 2)$ , where  $B_0^{12} = \{p_6\}$ . We get  $\mathcal{S}' = \{5\}$  at step 11 of Algorithm 4. We build a Steiner tree  $T_{2,\mathcal{S}}^{(13)}$  on  $G$  (Figure 28) with pivot at 2 and set of terminals  $\mathcal{S} = \{2, 5\}$ . Then flipping and traversing we get the following sequence of gates and row operations.

$$\begin{aligned}
\mathcal{Y} &= \{\text{CNOT}_{52}\} \\
\mathcal{A} &= \{B[5, .] \leftarrow B[5, .] \oplus B[2, .]\}
\end{aligned}$$

The updated  $B$  and the appended circuit has been shown in Figure 29. The column  $p_6$  is fixed, so we remove it from  $B$ . Now  $P_{76} = 1$  and we see that the circuit has the bit flip variable set to 1. The coefficient  $P_{86} = 7$ , so we place  $T^\dagger$  at the place where the 6<sup>th</sup> parity in  $P$  is realized. Now the stack is  $\mathcal{K} = \{(B_1^{12}, I \setminus \{2, 1, 3, 4\}, 2)\}$ .

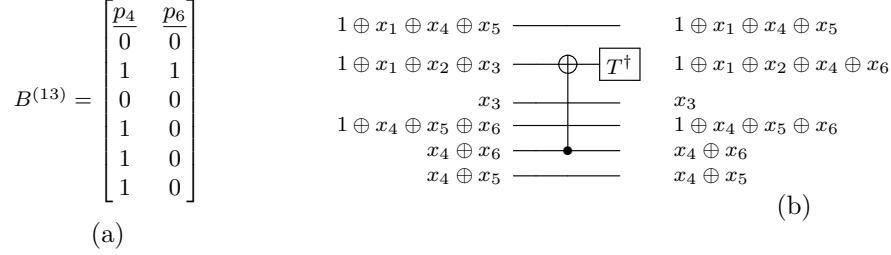


Figure 29: (a)  $B$  after applying row operations in iteration 13. (b) The partial circuit obtained after applying the gates obtained from iteration 13. The variables on the left and right denote the parities before and after the application of the gates respectively.

#### Iteration 14

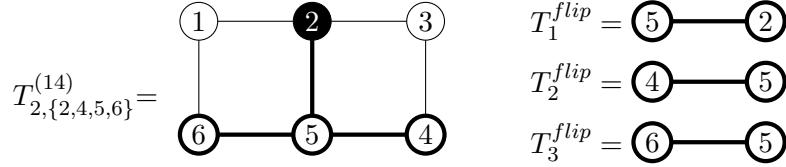


Figure 30: The Steiner tree  $T_{2,\{2,4,5,6\}}^{(14)}$  and its sub-trees, flipped such that root becomes leaf and vice-versa (iteration 14).

We pop  $(B_1^{12}, I \setminus \{2, 1, 3, 4\}, 2)$  from  $\mathcal{K}$ , where  $B_1^{12} = \{p_4\}$ . Now  $\mathcal{S}' = \{4, 5, 6\}$ . So we build a Steiner tree  $T_{2,\mathcal{S}}^{(14)}$  on  $G$  (Figure 30) with pivot at 2 and set of terminals  $\mathcal{S} = \{2, 4, 5, 6\}$ . After flipping the 3 sub-trees and traversing according to ROW-OP (Algorithm 2) we get the following sequence of CNOTs and row operations.

$$\begin{aligned} \mathcal{Y} &= \{\text{CNOT}_{65}, \text{CNOT}_{45}, \text{CNOT}_{52}\} \\ \mathcal{A} &= \{B[6, .] \leftarrow B[6, .] \oplus B[5, .], B[4, .] \leftarrow B[4, .] \oplus B[5, .], B[5, .] \leftarrow B[5, .] \oplus B[2, .]\} \end{aligned}$$

The state of  $B$  and the appended circuit has been shown in Figure 31. We find that the remaining column  $p_4$  has been fixed. Depending upon the parity realized and the coefficient (obtained from  $P$ ) we place a Z gate at the appropriate position in the circuit.

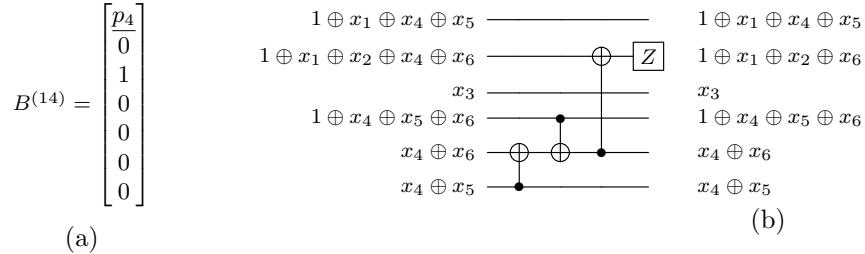


Figure 31: (a)  $B$  after applying row operations in iteration 14. (b) The partial circuit obtained after applying the gates obtained from iteration 14. The variables on the left and right denote the parities before and after the application of the gates respectively.